

CIPHERMAIL EMAIL ENCRYPTION

Ciphermail Gateway Administration Guide



April 4, 2016, Rev: 10215

Copyright © 2008-2016, ciphermail.com.

Acknowledgements: Thanks goes out to Andreas Hödle for feedback.

Contents

1	Introduction	6
2	Setup	6
3	Network	7
3.1	Network interfaces	7
3.2	Hostname	8
3.3	DNS	9
3.4	Hosts	9
3.5	NTP	9
4	MTA setup	10
4.1	Main settings	11
4.2	Advanced settings	14
4.3	sasl passwords	16
4.4	MTA config file	16
4.5	RBL	17
4.5.1	Static black-list	17
4.5.2	Static white-list	18
4.6	Email forwarding	18
4.7	Header checks	18
4.8	SMTP transports	19
5	Users	21
5.1	User preferences	21
5.1.1	General	23
5.1.2	S/MIME	24
5.1.3	PGP	26
5.1.4	PDF	26
5.1.5	Password (R)	27
5.1.6	Encryption subject trigger	27
5.1.7	Signing	28
5.2	Advanced settings	28
5.2.1	General	28
5.2.2	S/MIME	30
5.2.3	PGP	31
5.2.4	PDF	33
5.2.5	Encryption header trigger	35
5.2.6	Signing header trigger	35
5.2.7	Signing subject trigger	36
5.2.8	Password	37
5.2.9	One time password (OTP)	37
5.2.10	Security info	37
5.2.11	Subject filter	37
5.2.12	CA	37
5.2.13	Other	38
5.3	Global advanced settings	38
5.3.1	Security info	38

5.3.2	Subject filter	39
5.4	Mobile	39
5.5	SMS	40
5.6	Portal	41
5.7	PDF settings	42
5.7.1	Cover page	43
5.7.2	Attachments	43
5.7.3	Portal	44
5.7.4	Other settings	44
5.8	Webmail	44
5.8.1	Webmail settings	45
5.8.2	Webmail tunnel certificate	46
6	Domains	47
7	Templates	47
8	Certificates	50
8.1	Importing Certificates	52
8.2	Importing keys	52
8.3	Download certificates and keys	54
9	S/MIME	54
9.1	PKI	54
9.2	X.509 certificate	54
9.3	Revocation checking	57
10	Certificate selection	57
10.1	Encryption certificate selection	57
10.2	Signing certificate selection	59
10.3	Additional certificates	59
11	Certificate Revocation List	60
12	Certificate Trust List	61
13	Certificate Authority (CA)	63
13.1	Create new CA	64
13.2	CA settings	66
13.3	Certificate Request Handlers	67
13.3.1	built-in certificate request handler	68
13.3.2	delayed built-in certificate request handler	68
13.4	Create new end-user certificate	68
13.5	Select default CA	70
13.6	Pending requests	71
13.7	Bulk request	71
13.8	Create CRL	71
13.9	Send certificates	74

14 OpenPGP	76
14.1 Importing keys	76
14.2 Creating keys	77
14.3 Search keys	77
14.4 Key servers	77
14.5 Key details	79
14.6 Key trust	79
14.7 Publish public key	79
14.8 Email addresses	79
14.8.1 domains	80
14.9 Revoke key	80
14.10 Key selection	80
14.10.1 Email encryption key	81
14.10.2 Email signing key	81
15 PDF encryption	82
15.1 Encrypted PDF message	85
15.2 Replying	85
16 DLP	85
17 SMS gateway	87
17.1 Clickatell transport	87
18 Mail Queues	89
19 Logging	90
20 Administrators	90
20.1 Roles	90
21 Backup and restore	93
21.1 System backup	93
21.2 Backup configuration	93
21.2.1 SMB share settings	94
21.2.2 Automatic backup	94
21.2.3 Other	94
22 Log export	96
22.1 Log export config	96
22.1.1 SMB share settings	96
22.1.2 Automatic log export	98
22.1.3 Other	98
23 Reporting	98
23.1 Report	98

24 SSL/TLS	99
24.1 Web GUI	99
24.2 SMTP	99
24.3 CSRs	101
24.3.1 CSR manager	101
24.3.2 Certificate request procedure	102
25 Remote monitoring	103
25.1 Monitoring configuration	104
26 Certificate request by mail	104
26.1 Certificate request by mail reply templates	105
27 Proxy	105
28 Fetchmail	106
28.1 Fetchmail manager	107
28.1.1 Global settings	107
28.1.2 Applying changes	107
28.1.3 Adding a new account	107
29 System runtime control	109
30 Compose test email	109
31 Extract text from a MIME message	109
A SMTP HELO/EHLO name	113
B SASL authentication	113
C Content and virus scanning	115
D Cron Expressions	117
E MPA mail flow	118
F Comodo certificate request handler	138
F.1 Tier details	138
G Bulk import	138
G.1 Examples CSV	140

1 Introduction

Ciphermail email encryption server is an email gateway (MTA) that encrypts and decrypts your incoming and outgoing email. Because the Ciphermail gateway functions 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. The gateway is typically installed as a “store and forward” server. Email is therefore only temporarily stored until it is forwarded to its final destination.

The Ciphermail gateway currently supports three encryption standards: S/MIME, OpenPGP and PDF encryption. S/MIME and OpenPGP provides authentication, message integrity and non-repudiation and protection against message interception (using encryption). S/MIME and OpenPGP uses public key encryption (PKI) for encryption and signing. PDF encryption can be used as a light-weight alternative to S/MIME and OpenPGP. The PDF standard allows PDF documents to be password encrypted. PDF documents can also contain attachments embedded within the encrypted PDF.

Certain features are only available with the enterprise edition of the Ciphermail gateway. Where applicable, it will be clearly indicated whether a feature is an enterprise only feature.

Note

This guide provides in-depth information about the gateway appliance. For a quick setup guide of the gateway appliance, see the “CipherMail quick setup guide”.

2 Setup

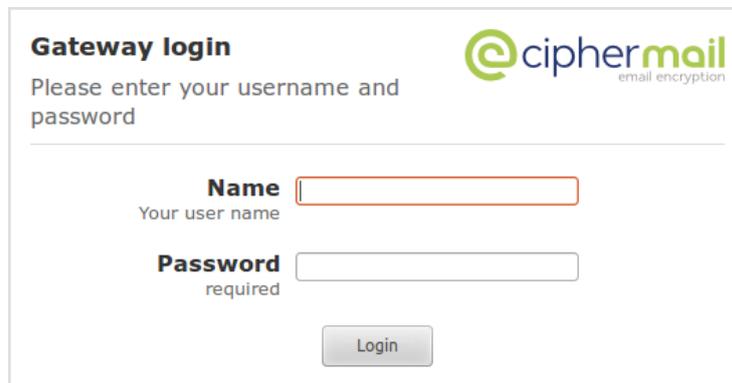
This guide assumes that Ciphermail gateway has already been installed. For installation instructions see the “installation guide”. The administrator can login to the administration page by opening the following URL in a browser: <https://192.168.1.1> (change the IP address to to match the address of the gateway).

Note: If the Ciphermail gateway was manually installed (i.e., not using the Virtual Appliance) the URL should probably be <https://192.168.1.1:8443/ciphermail>.

The login page should appear (See figure 1). After logging in with the correct credentials, the “users” page will be opened.

Login credentials: Use the following default credentials:

username: admin
password: admin



Gateway login 
Please enter your username and password

Name
Your user name

Password
required

Login

Figure 1: Login dialog

Note: it can take some time to login after a restart because the web application must be initialized upon first login.

3 Network

Note: The network settings page is only available for the Ciphemail Virtual Appliance. If the gateway has been manually installed, the network should be configured with the tools provided by the operating system.

Since the gateway needs to relay email to external recipients, the DNS servers should be configured. The network settings can be configured from the WEB GUI. The network info page can be opened by clicking Admin → network. The “Network info” page will be opened which provides all the relevant network information like DNS servers, network interfaces etc. (see figure 2).

Note: Since most network settings should be configured from the WEB GUI, the WEB GUI should have a valid IP before the WEB GUI can be accessed. A valid IP address can be setup with the console system application by logging into the console. See the “Virtual Appliance Guide” for more information.

3.1 Network interfaces

The available network interfaces can be configured by clicking “interfaces”. This opens the interfaces page (see figure 3). A network interface can be configured by clicking the “gear” icon of the interface. The network interface can be configured for a dynamic IP address (DHCP) or for a static IP address (see figure 4

Network info

[info](#) | [interfaces](#) | [hostname](#) | [DNS](#) | [hosts](#) | [ntp](#)

Network configuration information.

DNS servers

192.168.1.1

DNS domain list search

Network interfaces

Name	Address	MAC	Broadcast	Mask	Gateway	DHCP
eth0	192.168.1.109	00:15:5d:b2:2a:1d	192.168.1.255	255.255.255.0		true

Default gateway

192.168.1.1

Close

Figure 2: Network info

Network interfaces

[info](#) | [interfaces](#) | [hostname](#) | [DNS](#) | [hosts](#) | [ntp](#)

Manage network interfaces.

Network interfaces

Name	Address	MAC	Broadcast	Mask	Gateway	DHCP
eth0	192.168.1.109	00:15:5d:b2:2a:1d	192.168.1.255	255.255.255.0		true

Close

Figure 3: Network interfaces

3.2 Hostname

With the hostname page, the hostname of the gateway can be set (see figure 5). The hostname is used by many of the networking programs to identify the machine.

Note: It's advised to use a fully qualified hostname.

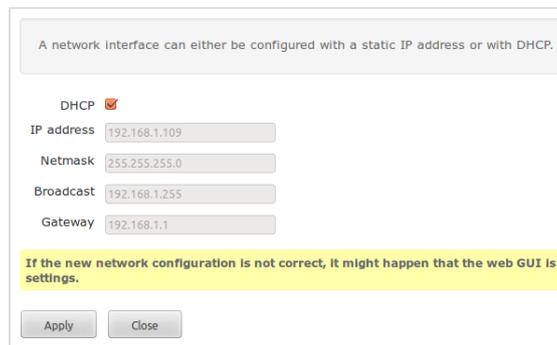


Figure 4: Network interface

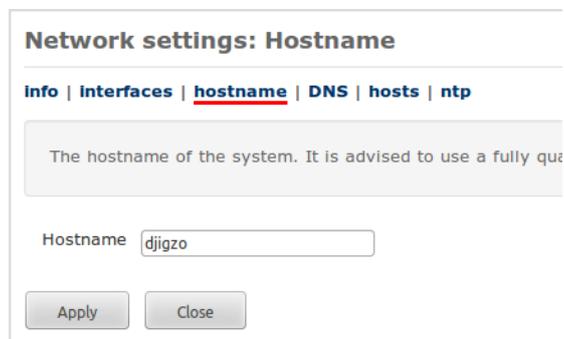


Figure 5: Hostname

3.3 DNS

The gateway requires at least one DNS server. The DNS server can be configured with the DNS page (see figure 6)

3.4 Hosts

The hosts table is a static lookup table for hostnames (see figure 7. In most setups, there is no need to add a static hostname to the hosts table. When the hostname (see hostname setting) is changed, the hosts table is automatically updated.

3.5 NTP

The gateway uses the Network Time Protocol (NTP) to keep the system clock synchronized with the real time. By default it uses the NTP servers from `debian.pool.ntp.org` (see figure 8. If you are running your own NTP server, change this to match the IPs or hostnames of the NTP servers.

Network settings: DNS

[Info](#) | [Interfaces](#) | [hostname](#) | [DNS](#) | [hosts](#) | [ntp](#)

On this page, the static DNS configuration can be set*. The DNS:

DNS 1

DNS 2

DNS 3

Domain search
domain suffix search
(space separated)

* The configured DNS servers on this page have a higher priority than the system's default DNS servers.

Figure 6: DNS

Network settings: Hosts

[Info](#) | [Interfaces](#) | [hostname](#) | [DNS](#) | [hosts](#) | [ntp](#)

The hosts file associates IP addresses with hostnames. For each IP address, you can specify one or more hostnames and aliases. The format is:

IP-address canonical-hostname [aliases...]

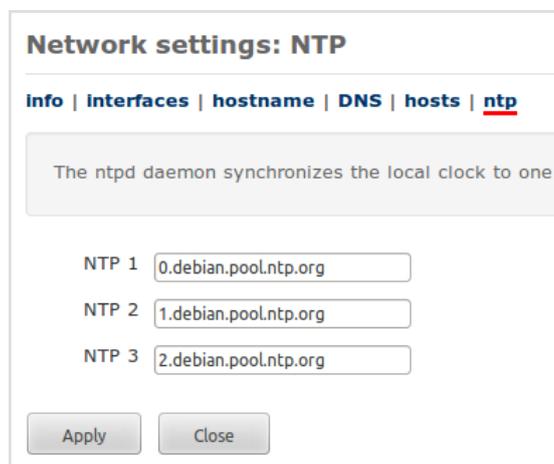
Hostnames and aliases should be separated by spaces. Up to 255 characters are allowed.

IP address	Hostnames & Aliases
<input type="text" value="127.0.0.1"/>	<input type="text" value="djigzo localhost"/>
<input "::1"="" type="text" value=""/>	<input type="text" value="ip6-localhost ip6-loopback"/>
<input type="text" value="fe00::0"/>	<input type="text" value="ip6-localnet"/>
<input type="text" value="ff00::0"/>	<input type="text" value="ip6-mcastprefix"/>
<input type="text" value="ff02::1"/>	<input type="text" value="ip6-allnodes"/>
<input type="text" value="ff02::2"/>	<input type="text" value="ip6-allrouters"/>
<input type="text"/>	<input type="text"/>

Figure 7: Hosts

4 MTA setup

The CIPHERMAIL gateway uses Postfix as the “Mail Transfer Agent” (MTA). The MTA is responsible for sending and receiving email. Encryption and decryption of email is handled by the “Mail Processing Agent” (MPA). The “MTA config” page can be used to configure most of the relevant Postfix parameters.



Network settings: NTP

[Info](#) | [interfaces](#) | [hostname](#) | [DNS](#) | [hosts](#) | [ntp](#)

The ntpd daemon synchronizes the local clock to one

NTP 1

NTP 2

NTP 3

Figure 8: NTP

The “MTA config” page can be opened from the Admin menu. The “MTA config” page (see figure 9) contains most of the relevant Postfix parameters for a “store and forward” email server. Postfix parameters which cannot be set with the “MTA config” page should be set with the “MTA raw config page” (or alternatively by directly editing the Postfix configuration files). The relevant Postfix settings will be explained in the following section. For a more thorough explanation of all the Postfix settings see the Postfix documentation (<http://www.postfix.org/documentation.html>).

4.1 Main settings

Relay domains Relay domains are domains for which the gateway needs to receive email. These are the domains for which the internal users receive email. A “store and forward” server normally has one or more relay domains (unless the Ciphermail gateway is only used for sending email).

Note: If “Match Subdomains” is selected (see other settings), subdomains of the relay domains are matched as well. If “Match Subdomains” is not selected, subdomains of the relay domains only match if the subdomains are explicitly added to the relay domains. For most setups, it is advised to explicitly add all the subdomains for which email should be received and leave “Match Subdomains” off.

Example: if “Match Subdomains” is selected, and example.com is added to the relay domains, then incoming email for the domain subdomain.example.com is accepted as well even if subdomain.example.com is not explicitly added to the relay domains.

My networks Most email senders (users and other internal email servers) are not allowed to send email to domains not specified as a “relay domain”.

MTA configuration

MTA config file

Relay domains

Relay domains
destination domains this system will relay mail to (and subdomains if Match Subdomains is selected)

Add domain
add a new relay domain

My networks

My networks
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
the internet hostname of this mail system

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

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

Match Subdomains
select if subdomains of Relay domains should automatically match

show advanced settings

Figure 9: MTA config

To allow outgoing email to be sent to external domains, the sender IP address should be “white-listed”. The “My networks” list contains all the networks that are allowed to send email to external domains. The networks must be specified in CIDR notation. **Example:** 192.168.1.1/32, 10.1.2.0/24.

Warning

Only allow IP ranges under your control to relay email to external recipients. If IP ranges not under your control are allowed, the gateway will be an open relay and misused for sending spam.

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. For example “My Hostname” is used as the default domain for email messages sent with a missing domain name and is used for the default SMTP helo/ehlo name (see “SMTP helo name” setting below).

If the gateway directly delivers email to external recipients (i.e., not using an external relay host) it is important that the helo/ehlo name of the gateway is equal to the reverse lookup of the external IP address. If not, outgoing email can be flagged as spam. See Appendix A for more information.

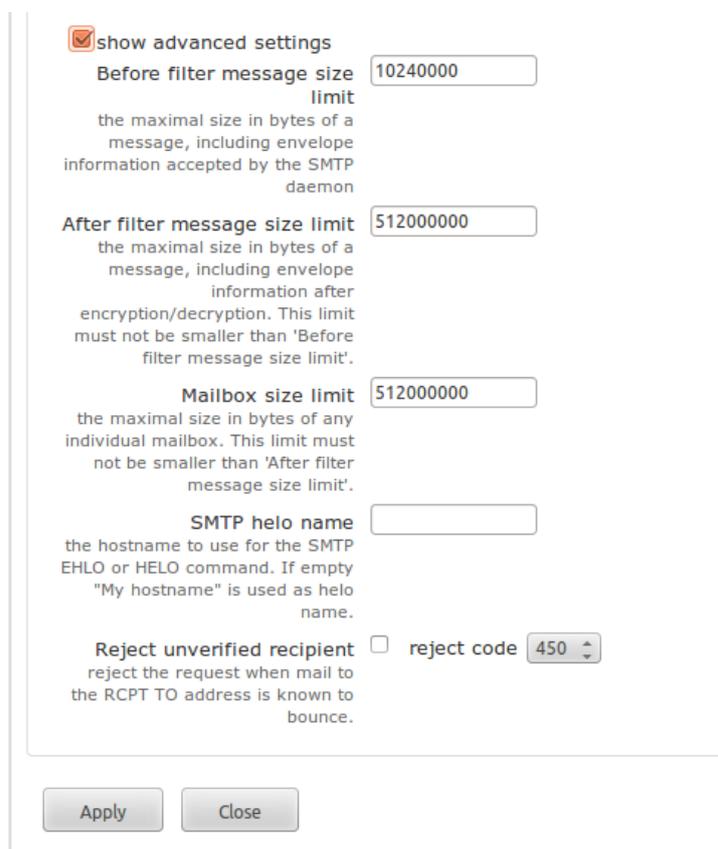
External relay host The external relay host is used when email should be sent to an external domain (i.e., a domain which is not a relay domain). This can be the ISPs email server or some internal email server responsible for sending email to external domains.

If “External relay host” is not specified, email will be delivered using DNS MX-records. “External relay host” can be an 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 the default SMTP port 25).

Internal relay host The internal relay host is used when email should be sent to an internal domain (i.e., sent to a relay domain). Typically this will be the companies internal email server hosting the users email boxes.

If “Internal relay host” is not specified, email will be delivered using DNS MX-records. “Internal relay host” can be an 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 the default SMTP port 25).

Match Subdomains If “Match Subdomains” is selected, all subdomains of the “Relay domains” will also be relayed.



show advanced settings

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

After filter message size limit
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
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 use for the SMTP EHLO or HELO command. If empty "My hostname" is used as helo name.

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

Figure 10: MTA advanced config

4.2 Advanced settings

The advanced settings can be set when the “advanced settings” checkbox is selected (see figure 10).

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.

Note: Because of Base64 encoding, binary attachments (for example word documents) will be 4/3 times larger if sent by email. The maximum size limit, limits the total number of bytes including encoding. For example, if the limit is set to 10 MB, the total size of all the attachments cannot exceed 7.5 MB.

After filter message size limit The mail processing agent of the gateway is responsible for encryption and decryption of messages. The size of a message after encryption or decryption (or after signing) can be larger than the size of the message before encryption or decryption. The “after filter message size

limit” should therefore be larger than the “before filter message size limit” otherwise the MTA will refuse to send the message after the MPA has handled the message. It is advised that the “after filter message size limit” should be at least 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 the gateway does not enable the option to directly specify local domains.

SMTP helo name The “SMTP helo name” is the hostname used for the SMTP “EHLO” or “HELO” command. If “SMTP helo name” is not explicitly specified, “My Hostname” is used as the SMTP helo name.

Note: If the gateway directly delivers email to external recipients (i.e., not using an external relay host) it is important that the helo/ehlo name of the gateway is equal to the reverse lookup of the external IP address. If not, outgoing email can be flagged as spam. See Appendix A for more information.

Reject unverified recipient Normally an email server should know which internal email addresses are valid addresses (i.e., email addresses for which an inbox exists). When an email server is setup to relay email for certain 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, there is a risk of generating “backscatter” bounces. Backscatter bounces, occur when an intermediate email server accepts a message without checking whether the next email server accepts the message. Because the intermediate email server accepted the message, it has to be bounced back to the original sender when the next server does accept the forwarded email. If the email was a spam message using a forged sender, the sender will be flooded with bounced messages.

There are multiple ways for an email server to know which recipient addresses are acceptable and which are not. One solution is to let the gateway server “learn” which recipient addresses are acceptable by querying the server it relays to. When an email is received for a yet unknown recipient, the server “asks” the server it relays to whether the recipient is a valid recipient or not. The message is only accepted when the next email server reports that the recipient is a valid recipient. The result of this verification process is cached.

The verification procedure is enabled by checking “Reject unverified recipient”. The “reject code” is the SMTP result code used when the email is not accepted. This should initially be set to “450” (which tells the connecting SMTP server that the message is not accepted because of a temporary error). It should be changed to “550” (permanent error) when the verification procedure

	Server	Port	Mx Lookup	Username	Password
<input type="checkbox"/> ✗	smtp.gmail.com	587	false	test	***

* smtp client authentication is only active when sasl is enabled.

Figure 11: SASL passwords

works correctly. See the Postfix documentation for more information on address verification¹.

There are other ways for the email server to know which recipients are valid, for example using LDAP queries or by specifying `relay_recipient_maps`. These other options are however not directly supported by the “MTA config” page and should therefore be configured using the “MTA raw config” page or by directly editing the Postfix configuration files.

Applying changes By clicking the “Apply” button, the changes will be checked and Postfix will be configured with the new settings. Clicking the “Close” button will redirect the browser to the “Admins” page.

4.3 sasl passwords

In cases where the “external relay host” or “internal relay host” requires SMTP authentication, a SASL account should be added. For example, if Gmail is used as the “external relay host”, the Gmail smtp server requires that the sender authenticates itself with the correct Gmail credentials. SMTP credentials for a specific host can be added by clicking *sasl passwords*. This opens the SASL passwords page (see figure 11).

SMTP password authentication is only active when SASL is enabled. For more information on how to enable SASL see Appendix B.

4.4 MTA config file

Postfix has a large number of settings. The “MTA config” page only supports a small number of the relevant Postfix settings. For settings not supported by the “MTA config” page, the “MTA config file” page can be used to directly edit the Postfix main config file (`main.cf`). The configuration file contains some specific CIPHERMAIL gateway settings (settings that start with “`djigzo_`”). These settings are modified by the “MTA config” page when applying the changes. These settings should therefore not be manually changed because they can

¹See http://www.postfix.org/ADDRESS_VERIFICATION_README.html

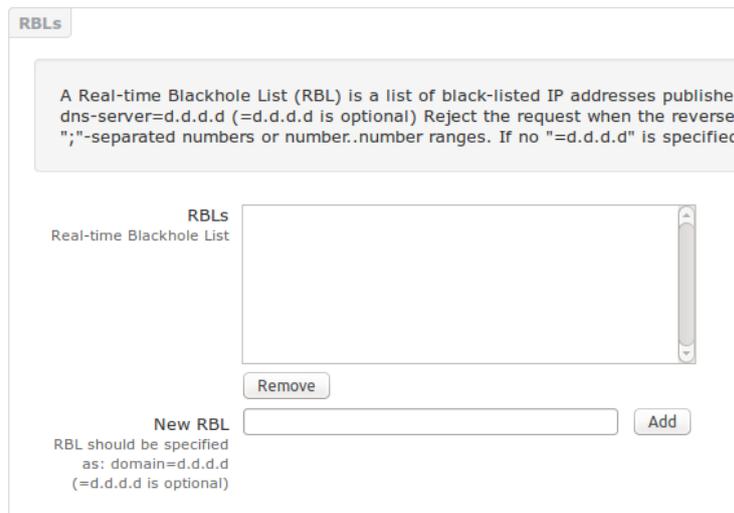


Figure 12: RBLs

be overwritten by the “MTA config” page. Ciphermail specific settings are used by other Postfix settings (they are referenced as “\${dijgzo_...}”).

Warning: The gateway does not validate any changes made to the “MTA config file” so care must be taken when modifying the Postfix config file directly. If the Postfix configuration file contains errors, Postfix might not function properly.

4.5 RBL

only available with the enterprise edition

A Real-time Blackhole List (RBL) is a list of black-listed IP addresses published by a DNS server. The MTA dynamically checks whether an external client is black-listed by querying a DNS server. The MTA rejects the request if the client IP address is listed in the DNS server. The list of RBL servers is shown in the RBLs section (see figure 12)

The RBL server should be specified as `dns-server[=d.d.d.d]`. The “=d.d.d.d” part is optional and depends on the used RBL whether or not the optional part should be specified.

4.5.1 Static black-list

The static black-list contains a list of black-listed clients. The difference between the static black-list and the RBL list is that the RBL dynamically checks whether a server is black-listed by querying an external DNS server. The static black-list is a list of IP addresses (or IP ranges) that are black-listed (see figure 13).

Figure 13: Static black-list

A range of IP addresses can be specified by leaving out the last octets from an IP address. For example: 192.168.88 will black-list all the IP addresses from 192.168.88.0 - 192.168.88.255. An optional rejection reason can be specified like for example “your IP was black listed because it is being used for sending spam”.

4.5.2 Static white-list

Static white-list list contains a list of white-listed IP addresses. An external client should be white-listed if incoming email should be accepted even though the client is black-listed by one of the configured RBL servers.

4.6 Email forwarding

only available with the enterprise edition

Forwarding of local system accounts to external email addresses can be configured on the email forwarding page (see figure 14). If root@domain forward is not set, system generated email will be sent to root@“My Hostname” (see MTA config for “My Hostname”).

Note: RFC 2142 requires that Internet facing SMTP servers accept email for the local postmaster and abuse account. If left empty, email for postmaster and abuse will be forwarded to the root account.

4.7 Header checks

only available with the enterprise edition

Email forwarding

On this page, forwarding of local accounts to external email addresses can be set.
If root@domain forward is not set, system generated email will be sent to root@My Hc

Forwards

root@domain
for system generated email

postmaster@domain*
for the local postmaster account

abuse@domain*
for the local abuse account

* RFC 2142 requires that Internet facing SMTP servers accept email for the local postm

Apply Close

Figure 14: Email forwarding

With header checks, each message header is matched against the list of defined patterns (see figure 15). If a pattern matches, the action for the pattern is executed. For the matching and action syntax, see the Postfix header checks documentation (http://www.postfix.org/header_checks.5.html)

Example: The following rule will reject the email if the subject line of the email starts with “make money fast”:

```
/^Subject: make money fast/ REJECT spam detected
```

4.8 SMTP transports

only available with the enterprise edition

By default all email sent to external recipients (i.e., email addresses not matching any relay domain) will be delivered to the “External relay host” or, if “External relay host” is not configured, it will be delivered using MX records. In a similar way, email sent to one of the relay domains will be delivered to the “Internal relay host” or, if “Internal relay host” is not configured, it will be delivered using MX records. SMTP transports allow the administrator to override the default mail delivery. For example, if CipherMail Secure Webmail is used, email for the webmail domain should be delivered directly to the Secure Webmail server. Although it’s possible to configure an MX record for the webmail domain, in most cases it’s easier to configure an SMTP transport for the webmail domain. The list of SMTP transports can be managed on the SMTP transport page (see figure 16).

Header checks

These header checks are applied to the initial message headers.

Header checks

Header check rules

Apply Close

Figure 15: Header checks

SMTP transports

Optional lookup tables with mappings from recipient domain to message del
If use MX is set, the MX record for the relay host will be looked up to find th

add transport

	Recipients domain	Relay Host	Use MX
✘	webmail.local	192.168.88.188	false

Close

Figure 16: SMTP transports

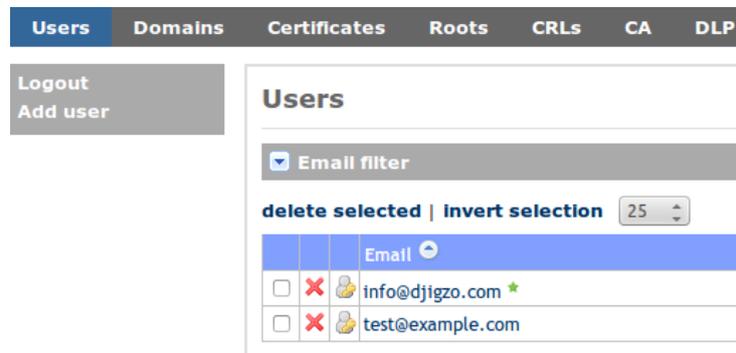


Figure 17: Users

5 Users

A user is a sender or receiver of email and is uniquely identified by his/her email address. Every user has a set of preferences that determine how email is handled for that particular user. The users page gives an overview of all the users (see figure 17).

Specific users can be searched for using the filter. Users can be removed by clicking the 'cross' icon or by selecting the 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 page (see next section). Internal users are marked with a green star icon (see "Locality property" on page 23 for more info on the difference between 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 user is an external user, the "select encryption certificates" page is opened.

5.1 User preferences

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 their preferences from domain preferences, domain preferences inherit from the global preferences and the global preferences inherit from the factory preferences:

user ← domain ← wild-card domain² ← global ← factory.

The preferences for a user can be edited by clicking on the users email address (see figure 18). The user preference page links to sub-pages "select encryption certificates", "select signing certificate", "templates" and "global preferences" which can be used to edit additional preferences. Whether a preference is inherited or not is determined by the associated "inherit" checkbox. If checked, the preference is inherited.

²An example of a wild-card domain is *.example which matches test.example.com.

Edit user: info@ciphemail.com

[S/MIME](#) | [PGP](#) | [portal](#) | [templates](#) | [DLP](#) | [sms](#)

General

Comment inherit

Locality inherit

Encrypt Mode inherit

Encryption notification inherit

S/MIME

Enabled inherit

Strict mode inherit

Max. message size (bytes) inherit

PGP

Enabled inherit

PGP encoding to external inherit

Enable PGP/INLINE to internal inherit

Max. message size (bytes) inherit

PDF

Enabled inherit

OTP enabled inherit

Generate password to originator inherit

Max. message size (bytes) inherit

Password

Password inherit

Password ID inherit

Validity interval (min) inherit

Encryption subject trigger

Trigger inherit

Enabled inherit

Regular expr. inherit

Remove match inherit

Signing

Only sign when encrypt inherit

show advanced settings

Figure 18: User preferences

Sender and receiver preferences Some preferences are only relevant for the sender of a message and some preferences are only relevant for the receiver of a message. Most preferences however are relevant for both the sender and receiver. The MPA mail flow in Appendix E shows exactly when and how preferences are used by the MPA.

Note: “S” or “R” (surrounded by parentheses) is placed after the property name to indicate whether a preference is a sender preference or a receiver preference. Some properties are used as a sender and receiver property. A property which is used as a sender or recipient property is written as (S | R). A property which is used as a sender and recipient property is written as (S & R).

Message originator The Ciphermail gateway uses the “From” header as the identity of the sender and not the “envelope sender”. It is important to understand the difference between the from and the envelope sender because the identity of the sender determines which settings and certificates will be used by the sender. Because sender is such a confusing term, the term “originator” will be used instead when referring to the identity of the sender (i.e., the from header).

The rationale for using the “From” for the identity of the sender is that the envelope sender is more or less similar to the postman and is therefore only responsible for the message delivery and not for the message content whereas the “From” identifies the actual originator of the email. The user identified by the “From” is responsible for the message content. In most cases however, the envelope sender is the same as the “From”.

Another important reason why the from header is used, is that S/MIME uses the from header as the identity of the sender, i.e., an S/MIME client compares the email address of the signing certificate with the from header of the message. While the identity of the sender is determined by the from header, the identity of the recipient is determined by the recipient of the SMTP envelope and not the “To” header.

Next, a brief overview of the all the user preferences will be given.

5.1.1 General

Comment This field is a free form text field in which the administrator can add some comments related to this user.

Locality (R) The “locality” of a user can be external or internal. The “locality” preference is a very important preference because it determines whether email coming into the gateway should be encrypted or decrypted. If the recipient of an email is an internal user, the email should be decrypted. If the recipient of an email is an external user, the message should be encrypted (whether the message will actually be encrypted depends on other user settings). Typically users for which the gateway receives email will be internal users (i.e., users

belonging to one of the relay domains) 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” header³.

Note: because the locality is such an important preference, it should be setup correctly. In most installations all domains for which the gateway receives email (i.e., the relay domains) should be internal domains. By default all users and domains are external.

Encrypt mode (S & R) Encrypt mode determines whether a message sent to an external user (i.e., a user with external locality) should be encrypted or not. The possible encrypt modes are: “No Encryption”, “Allow”, “Mandatory” and “Allow (sender or recipient)”. Encrypt mode is used for the sender and recipient (with the exception of Allow (sender or recipient)). If 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 or PDF encryption is setup for the recipient). 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.

Encrypt mode (except if the mode is Allow (sender or recipient)) is a sender and receiver preference. This means that the settings for both the sender and receiver must allow encryption. If for example the sender has encrypt mode “Mandatory” and 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 “Allow (sender or recipient)”, the other encrypt mode is ignored and encryption is allowed. “Allow (sender or recipient)” encrypt mode is for example used when all email sent to an external recipient should always be encrypted regardless of the “Encrypt mode” of the sender.

Encryption notification (S) If set, the sender of the message will be notified (with an email) when the message is encrypted (see template “successful encryption” on page 50 for the notification message template).

5.1.2 S/MIME

Enabled (S & R) If checked, digital signing and encryption of outgoing email with S/MIME is supported.

Strict mode (R) By default, the gateway tries to decrypt every incoming S/MIME encrypted message even if the recipient of the message does not have an associated private key with which the message can be decrypted. In other words, the gateway tries to decrypt the message with any suitable key (“decrypt if possible”). There are a couple of advantages when decrypting every incoming email irrespective of the recipient: a) it makes it easier to manage domain to

³If there is no “From” header, the “Sender” header will be used. If the “Sender” header is also missing, the envelope sender will be used.

domain encryption; b) forwarded email can be decrypted and, c) email handling with multiple recipients is faster because only one key is required for decryption.

Even though non-strict mode is easier from a management perspective, it is not as secure as “strict” mode. In non-strict mode, if an external attacker gets hold of an encrypted message, the attacker can resend the message to an internal accomplice, i.e., someone from inside the company who has access to an internal mail box and who works closely with the attacker. Because the message will be decrypted with any available key, the message will be delivered decrypted to the insider even though the insider was not the original recipient.

In “strict” mode, additional checks will be done to make sure that the message will only be decrypted if the recipient has a valid decryption key. A message will only be decrypted for a recipient if the certificate associated with the private key for decryption is valid, trusted, not revoked and if one of the following is true:

- (a) the recipient has a certificate and private key with a matching email address and the message can be decrypted with this private key or,
- (b) the recipient has a certificate and private key and the certificate is explicitly associated with the user and the message can be decrypted with the private key or,
- (c) the recipient is from a domain and the domain has an explicitly associated certificate and private key and the message can be decrypted with this private key.

If in strict mode, every recipient for which none of the above rules apply, will receive the message in encrypted form.

Whether or not to use strict mode depends mostly on whether you trust your internal users. If you do not trust all internal users, it’s better to enable strict mode. If all internal users can be trusted, running in non-strict mode might be somewhat easier to manage.

Note: strict mode can be enabled and/or disabled per domain and per recipient. Although it’s advised to only change the global strict settings, there are situations where it can be helpful to enable or disable strict mode per recipient. For example, suppose the global strict mode is enabled. However, because of email archiving purposes, the front-end SMTP server sends a copy (bcc) of every incoming email to the email archiver. Since the gateway is in strict mode, encrypted message won’t be decrypted by the gateway when delivered to the email archiver. By disabling strict mode for the email archiver recipient, incoming email delivered to the email archiver will be decrypted.

Max. message size (S | R) If the email message is larger than the specified maximum message size (in bytes) the message will not be S/MIME signed or encrypted. Large S/MIME messages can sometimes not be handled by S/MIME email clients. Another reason for limiting the size of S/MIME messages is that encrypting and signing of large email messages can be resource intensive.

5.1.3 PGP

PGP enabled (S & R) If checked, PGP for outgoing email is supported.

PGP encoding to external (R) The PGP encoding used for outgoing email. Two encodings are supported: PGP/MIME and PGP/INLINE. PGP/MIME is advised because it secures the complete message MIME message and supports HTML email. With PGP/INLINE, every MIME part is individually PGP encoded. PGP/INLINE support for HTML email is limited and is not supported by all email clients.

Note: You are strongly advised to use PGP/MIME whenever possible. PGP/MIME has full support for HTML email and is less resource intensive.

Enable PGP/INLINE to internal (R) PGP supports two types of encoding: PGP/MIME and PGP/INLINE. With PGP/MIME, the complete MIME message is protected as one object. A PGP/MIME protected message can be easily recognized without having to scan the complete message because it contains a PGP/MIME specific header. With PGP/INLINE, every individual part of the message (attachments and message bodies) is individually protected (signed and/or encrypted). To determine whether or not a message is PGP/INLINE protected, the complete message must be scanned. A PGP/INLINE message does not contain a specific header which can be used to determine whether the message is PGP/INLINE protected. Scanning every incoming email completely from top to bottom can be resource intensive, especially for very large attachments. It is therefore advised to leave "Incoming PGP/INLINE enabled" unchecked (i.e., disabled) unless PGP/INLINE support for incoming email is a requirement.

Note: leave "Incoming PGP/INLINE enabled" unchecked (i.e., disabled) unless PGP/INLINE support for incoming email is a requirement.

Max. message size (S | R) If the email message is larger than the specified maximum message size (in bytes) the message will not be PGP signed or encrypted. Large PGP messages can sometimes not be handled by PGP email clients. Another reason for limiting the size of PGP messages is that encrypting and signing of large email messages can be resource intensive.

5.1.4 PDF

Enabled (S & R) If checked, PDF encryption is supported.

OTP enabled (S & R) With the one time password mode, passwords for PDF encryption will be generated based on the "Client Secret" and on the "Password ID". For more information on the OTP mode, see the PDF encryption guide). If selected, the one time password mode is enabled for the user.

Generate password to originator (S & R) If checked, generated passwords will be sent to the originator of the message (i.e., the sender) as a notification message. The notification message will contain the generated passwords (see template “passwords” on page 50 for the notification message template). The originator is responsible for delivering the generated passwords securely to the recipients of the encrypted message.

Max. message size (S | R) PDF encryption not only encrypts the message body but also encrypts the message attachments. To prevent the PDF from becoming too large, the PDF is not encrypted if the total size of body text and attachments exceeds the maximum message size (in bytes).

5.1.5 Password (R)

Password The password for the user. Currently this is only used for PDF encryption. The password can be set by the administrator or can be randomly generated. If the current password has expired (see “Validity interval”) a new password will be generated when the password is used. If a static password should be used, password expiration should be disabled by setting “Validity interval” to -1.

Password ID (R) The “Password ID” identifies the password used for PDF encryption. The “Password ID” is required when the “One Time Password” (OTP) mode is used or when the password is delivered by SMS Text.

With the OTP encryption mode, a password will be generated based on a secret key and on a unique identifier (the “client secret” and the “Password ID”). The “Password ID” is used by the recipient of the encrypted PDF message to regenerate the password (for more information about the OTP mode, see the PDF encryption guide). With the SMS Text mode, the randomly generated password will be delivered to the recipient via an SMS text message. Because the recipient can receive multiple passwords via SMS Text, the recipient has to know which password belongs to which encrypted PDF. The encrypted PDF messages therefore contain a password identifier which can be used to find the matching password. Every time a new password is generated, a new unique password ID is generated. The “Password ID” property shows the last generated password ID for the user.

Validity interval (R) The time (in minutes) the password is valid. If the password is no longer valid (expired) a new password will be generated when the password is used. 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.

5.1.6 Encryption subject trigger

A subject trigger can be used to force encryption if the subject contains a certain keyword. This is useful when the default setting for a sender or recipient is “No encryption” but the sender wants to force encryption of a particular message (“on demand encryption”).

Trigger (S) If the subject contains the provided trigger keyword and the subject trigger is enabled, encryption is forced for this message. Whether the message is really encrypted depends on the availability of valid certificates for the recipients. If encryption is triggered but the message cannot be encrypted, the message will not be sent and the sender will be notified.

Enabled (S) The subject trigger functionality will only be functional if “Enabled” is checked.

Regular expr. (S) If checked, “Trigger” is interpreted as a regular expression and the subject is matched against this regular expression.

Example: `(?i)(\[secure\]|\[encrypt\])`.

With the above subject trigger, encryption will be forced if the subject contains `[secure]` or `[encrypt]`. `(?i)` makes the check case insensitive.

Remove match (S) If checked, the matching part will be removed from the subject.

Example: Suppose the trigger is set to `"[encrypt]"` and the subject of the incoming message is `"your bank statement [encrypt]"` the subject after encryption is `"your bank statement"`.

5.1.7 Signing

Only sign when encrypt (S & R) If checked, messages will only be digitally signed when they are S/MIME or PGP encrypted. If not checked, all messages will be digitally signed. The sender of a message must have a valid signing certificate or PGP key before a message can be digitally signed. S/MIME signing is tried before PGP signing, i.e., if a sender has a valid S/MIME signing key, the message will be S/MIME signed. If the sender does not have a valid S/MIME signing key but has a valid PGP signing key, the message will be PGP signed.

5.2 Advanced settings

The advanced settings sub page contain settings which are only used in specialized setups (see figure 19). Some settings can only be set for the global settings. See 5.3 for more information on the global specific settings.

5.2.1 General

Skip calendar messages (S | R) If checked, calendar messages⁴ (for example Outlook meeting requests) are not digitally signed or encrypted. Some email clients, for example Outlook, cannot handle meeting requests if the meeting requests are digitally signed or encrypted.

⁴Messages with the content-type “text/calendar”

show advanced settings

General

Skip calendar messages inherit

S/MIME

Encryption algorithm 3DES inherit

Signing algorithm SHA1 inherit

Auto select certificates inherit

Always use freshest signing certificate inherit

Auto request certificate inherit

Add user inherit

Encrypt headers inherit

Remove signature inherit

Skip calendar messages inherit

Skip signing calendar messages inherit

Add additional certificates inherit

Auto import certificates from email inherit

Skip import of untrusted certificates inherit

PGP

Signing algorithm SHA256 inherit

Encryption algorithm AES-128 inherit

Compression algorithm ZLIB inherit

Convert HTML to text inherit

Add integrity packet inherit

Key size 2048 inherit

Auto publish inherit

Auto request inherit

Remove signature inherit

Import keys from email inherit

Remove keys from email inherit

Auto update email addresses inherit

PDF

Only if mandatory inherit

Sign email inherit

Reply allowed inherit

Send CC to replier inherit

Validity interval (min) inherit

Reply URL inherit

Reply sender inherit

Figure 19: Advanced user preferences

Note: Enabling “Skip calendar messages” does not result in skipping DLP.

5.2.2 S/MIME

Encryption algorithm (R) The encryption algorithm to use when encrypting the message. The following encryption algorithms can be selected: “AES256”, “AES192”, “AES128”, “3DES”, “RC2”, “CAST5”, “CAMELLIA256”, “CAMELLIA192”, “CAMELLIA128” and “SEED”.

Note: some S/MIME clients only support a subset of the available algorithms. For example Outlook only supports “AES256”, “AES192”, “AES128”, “3DES” and “RC2”. “3DES” is supported by all S/MIME clients.

Signing algorithm (R) The signing algorithm to use when signing the message. The following signing algorithms can be selected: “SHA1”, “SHA256”, “SHA512” and “RIPEMD160”.

Note: some S/MIME clients only support a subset of the available algorithms. In order to validate SHA2 (SHA256 and SHA512) messages, Windows Vista with Outlook 2003 (or newer) is needed. In order to both sign and validate SHA2 messages, Windows Vista or 7 with Outlook 2007 or 2010 is needed (see <http://blogs.technet.com/b/pki/archive/2010/09/30/sha2-and-windows.aspx>).

Auto select certificates (R) If checked, encryption certificates will be automatically selected for the recipient.

Always use freshest signing certificate (R) The first time a message must be signed, the gateway automatically searches for a valid signing certificate for the sender. Once a signing certificate has been selected, the signing certificate will be used for all signing operations until the certificate is no longer valid. If however “Always use freshest signing certificate” is selected, every time a message is signed, the newest signing certificate (i.e., a valid certificate with the latest “not before”) is used.

Auto request certificate (S) If checked and the sender does not yet have a valid signing certificate, a new certificate and private key will be automatically requested for the sender using the default Certificate Authority (see CA Settings on page 66).

Add user (R) If checked and a certificate is available for the recipient, a user object will be created if a message is S/MIME encrypted.

Encrypt headers (R) If checked, certain headers (“Subject”, “To”, “Cc”, “Reply-To” and “From”) are added to the encrypted message. This option is normally only used when encrypting email to a Ciphermail for Android user (it provides access to all the relevant headers from the smime.p7m attachment).

Note: the headers are added to the encrypted binary blob and are “not” removed from the message. Do not select this option if the recipient uses Outlook because Outlook does not support encrypted headers.

Remove signature (R) If checked and an incoming message is signed, the signature will be removed from the message. This can be helpful when the email client used by internal users or some email handling software cannot handle digitally signed messages.

Skip calendar messages (S | R) If checked, calendar messages⁵ (for example Outlook meeting requests) are not digitally signed or encrypted. Some email clients, for example Outlook, cannot handle meeting requests if the meeting requests are digitally signed or encrypted.

Skip signing calendar messages (S | R) If checked, calendar messages (for example Outlook meeting requests) are not digitally signed. Some email clients, for example Outlook, cannot handle meeting requests if the meeting requests are digitally signed. The difference between “Skip signing calendar” and “Skip calendar” is that when “Skip signing calendar” is checked but “Skip calendar” is not, messages can still be encrypted. This can be helpful when all email, including calendar messages, sent to a specific domain must be encrypted with a domain certificate.

Add additional certificates (S | R) If checked and the message is S/MIME encrypted, the message will also be encrypted with the additional certificates. See [10.3](#) for more information.

Auto import certificates from email (S) If checked, certificates from received digitally signed emails will be automatically extracted and stored in the certificates store.

Skip import of untrusted certificates (S) If checked, extracted certificates (see “Auto import certificates from email”) will only be imported if the certificates are trusted.

5.2.3 PGP

The PGP advanced options are shown in [Figure 20](#).

Signing algorithm (R) The signing algorithm to use when signing the message. The following signing algorithms can be selected: “SHA1”, “SHA256”, “SHA512” and “RIPE-MD/160”.

⁵Messages with the content-type “text/calendar”

PGP

Signing algorithm	SHA256	<input checked="" type="checkbox"/> inherit
Encryption algorithm	AES-128	<input checked="" type="checkbox"/> inherit
Compression algorithm	ZLIB	<input checked="" type="checkbox"/> inherit
Convert HTML to text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> inherit
Add integrity packet	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> inherit
Key size	2048	<input checked="" type="checkbox"/> inherit
Auto publish	<input type="checkbox"/>	<input checked="" type="checkbox"/> inherit
Auto request	<input type="checkbox"/>	<input checked="" type="checkbox"/> inherit
Remove signature	<input type="checkbox"/>	<input checked="" type="checkbox"/> inherit
Import keys from email	<input type="checkbox"/>	<input checked="" type="checkbox"/> inherit
Remove keys from email	<input type="checkbox"/>	<input checked="" type="checkbox"/> inherit
Auto update email addresses	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> inherit

Figure 20: PGP advanced user preferences

Encryption algorithm (R) The encryption algorithm to use when encrypting the message. The following encryption algorithms can be selected: “AES256”, “AES192”, “AES128”, “3DES”, “CAST5”, “Blowfish” and “Twofish”.

Compression algorithm (R) The compression algorithm to use when encrypting the message. The following compression algorithms can be selected: “UNCOMPRESSED”, “ZIB”, “ZLIB”, “BZip2”. If “UNCOMPRESSED” is selected, the message is not compressed before encryption.

Convert HTML to text (R) This option is only used if the message is PGP/INLINE encoded. Because there is no standard way to handle HTML email with PGP/INLINE, if “Convert HTML to text” is selected, HTML parts will be converted to text. This options is not used if the message is PGP/MIME encoded.

Add integrity packet (R) If set, an integrity packet will be added to the PGP encoded message.

Key size (S) The key size (in bits) of automatically generated secret PGP key pairs (see “Auto request” option). The following key size can be selected: 1024, 2048, 4096.

Auto publish (S) If checked, automatically generated PGP secret keys will be automatically published to the registered PGP key servers.

Auto request (S) If a message needs to be PGP encrypted and the sender does not yet have a valid PGP secret key, and auto request is set, a new PGP secret key will be generated for the sender.

Remove signature (R) If true, the PGP signature is removed from the message.

Import keys from email (R) If true, and a PGP key is attached with the content type set to "application/pgp-keys", the key will be imported.

Note: Inline attached keys are not currently not supported.

Remove keys from email (R) If true, and a PGP key is attached with the content type set to "application/pgp-keys", the key will be removed from the email.

Note: Inline attached keys are not currently not supported.

Auto update email addresses (S | R) If "Auto update email addresses" is selected, all the email addresses found in a valid User ID of a PGP key will be automatically associated with the key. Only User IDs with a valid self signed signature will be used. If "Auto update email addresses" is not selected, email addresses should be manually associated with the key. This is a global only option.

Note: Since a User ID is not validated, the key owner can add email addresses it does not own (it is only checked whether the User ID contains a valid self signature). If you want to make sure that only email addresses are added which you know are valid for the user, disable "Auto update email addresses" and manually associate the email addresses. Future versions of Ciphermail will support validation of User IDs by checking additional signatures.

5.2.4 PDF

A brief explanation of the advanced PDF preferences will be given. See the "PDF Encryption Guide" for more information on how to setup PDF encryption.

Only if mandatory (S | R) If checked, PDF encryption will only be enabled if encryption is mandatory (for example, if encrypt mode is mandatory, or encryption is triggered using the subject trigger).

Sign email (S & R) If checked and the sender has a valid signing certificate, the email containing the encrypted PDF will be S/MIME digitally signed⁶.

Reply allowed (S & R) If checked, the encrypted PDF will contain a "Reply" link which can be used by the recipient of the encrypted PDF to securely reply to the message using the built-in portal.

⁶The email containing the PDF is signed, not the PDF itself.

Send CC to replier (S & R) If checked, a CC of the PDF reply will be sent to the replying user.

Warning: To make sure that the CC sent to the replier is encrypted, set “Encrypt mode” of the “Reply sender” (see setting below) to “Mandatory”.

Validity interval (R) If checked, the “Validity interval” determines how long (in minutes) a reply link is valid.

Reply URL (S) A recipient can securely reply to the PDF by clicking the reply link in the PDF. The reply link opens the reply page of the built-in portal using the default web browser. The reply URL should be setup to link to the external URL of the PDF reply page. The default reply URL is based on the portal “Base URL” (see 5.6). It is therefore advised to change the “Base URL” of the portal and only change the “Reply URL” if the PDF reply page runs separately from the portal.

Reply sender (S) The envelope sender of the PDF reply message will be set to “Reply sender”. The local name part of the “From” header of the reply message will be set to the email address of the replying user prefixed with “in name of”.

Example: If the user `martijn@ciphemail.com` replies to the encrypted PDF using the reply portal page, the reply will contain the following from:

```
"in name of martijn@ciphemail.com" reply@example.com
```

(where `reply@example.com` is the “Reply sender” address and `martijn@ciphemail.com` is the email address of the user that replies).

The “Reply-To” header is set to the email address of the replier to make sure that a reply is sent to the correct recipient.

A reply using the reply portal page is always sent using the same sender because:

- (a) The reply sender is always a known address. The encryption rules for the reply sender can therefore be specified. For example, it’s possible to force all PDF reply messages to be encrypted.
- (b) If for some reason the reply message is bounced, the bounce will not be sent to the original sender but to the “Reply sender”. This prevents the bounced message from accidentally being sent over the Internet without encryption.
- (c) Using the real email address of the replying user as the envelope sender requires the gateway to “spooF” the sender address. If the sender domain of the replying user has defined any SPF records, the reply can be flagged as a forgery and therefore blocked by spam filters.

5.2.5 Encryption header trigger

Force encrypt allowed (S) If checked, senders are allowed to trigger encryption of messages with a specific header (see “Force encrypt trigger”).

Force encrypt trigger (S) The “Force encrypt trigger” can be used to trigger encryption of a message using a specific email header. All headers of an outgoing email are matched against the “Force encrypt trigger” and if there is a match, encryption is forced. If the header is present but the message cannot be encrypted, the message will be bounced back to the sender to notify that the message could not be encrypted.

Force encrypt trigger, for example, can be used when an automated system sends email to external recipients and some, but not all, emails should be encrypted. By adding a header to an outgoing email, the external system can specify whether the email should be encrypted or not.

The trigger is specified as: `HEADER[:REG_EXPR]`, where “HEADER” is the name of the header and “REG_EXPR” is the optional header value specified as a regular expression. If “REG_EXPR” is not specified, all header values are accepted. If “REG_EXPR” is specified, only those header values that match the regular expression will trigger encryption.

Examples: The following examples trigger encryption when the messages contains the X-Encrypt header. The header values are ignored (i.e., all header values are accepted).

```
X-Encrypt
X-Encrypt:
X-Encrypt:*
```

The following example triggers only when the message contains a header named X-Encrypt with a header value of “true” (whitespace is ignored and checks are case insensitive).

```
X-Encrypt:(?i)^\s*true\s*$
```

5.2.6 Signing header trigger

Force signing allowed (S) If checked, senders are allowed to trigger signing of messages with a specific header (see “Force signing trigger”).

Force signing trigger (S) The “Force signing trigger” can be used to trigger S/MIME signing of a message using a specific email header. All headers of an outgoing email are matched against the “Force signing trigger” and if there is a match, S/MIME signing is forced.

This can for example be used when an automated system sends email to external recipients and some, but not all, emails should be digitally signed. By adding a header to an outgoing email, the external system can specify whether the email should be signed or not.

The trigger is specified as: `HEADER[:REG_EXPR]`, where “HEADER” is the name of the header and “REG_EXPR” is the optional header value specified as a regular expression. If “REG_EXPR” is not specified, all header values are accepted. If “REG_EXPR” is specified, only those header values that match the regular expression will trigger signing the message.

Examples: The following examples trigger signing when the messages contains the `X-Sign` header. The header values are ignored (i.e., all header values are accepted).

```
X-Sign
X-Sign:
X-Sign:*
```

The following example triggers only when the message contains a header named `X-Sign` with a header value of “true” (whitespace is ignored and checks are case insensitive).

```
X-Sign:(?i)^\s*true\s*$
```

5.2.7 Signing subject trigger

A subject trigger can be used to force signing of a message if the subject contains a certain keyword. This is useful if the default setting for a sender or receiver is “Only sign when encrypt” (which means that the message won’t be signed by default), but the sender wants to force signing of the message (“on demand signing”).

Trigger (S) If the subject contains the provided trigger keyword and the subject trigger is enabled, signing is forced for this message. Whether the message is really signed depends on the availability of a valid signing certificate for the sender. If signing is triggered but the message cannot be signed for whatever reason, the message will not be signed.

Enabled (S) The subject trigger functionality will only be functional if “Enabled” is checked.

Regular expr. (S) If checked, “Trigger” is interpreted as a regular expression and the subject is matched against this regular expression.

Example: `(?i)\[\s*sign\s*\]`

With the above subject trigger, signing will be forced if the subject contains `[sign]`. `(?i)` makes the check case insensitive.

Remove match (S) If checked, the matching part will be removed from the subject.

Example: Suppose the trigger is set to "[sign]" and the subject of the incoming message is "your bank statement [sign]" the subject after encryption is "your bank statement".

5.2.8 Password

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

Date last generated (R) The date the password was generated. This is used in combination with the "validity interval" to determine whether the password is still valid. If "Date last generated" is empty, the password will never expire.

5.2.9 One time password (OTP)

OTP URL (R) The recipient of an OTP encrypted PDF, needs to access the portal to generate the password for the PDF. The default external URL for the OTP password generator is based on the portal "Base URL" (see 5.6).

Note: You are advised not to change the "OTP URL" but to change the "Base URL" of the portal. The only reason to change the "OTP URL", is if the OTP generator runs separately from the portal.

5.2.10 Security info

Add security info (R) If checked and an incoming email is S/MIME encrypted or signed, information about the encryption or signature will be added to the subject. For more information see 5.3.1.

5.2.11 Subject filter

If enabled, the subject of incoming email will be filtered with the filter setup on the global settings (see 5.3.2 for more information).

5.2.12 CA

Last used pfx password If a pfx file was generated, "Store password" was selected when generating the pfx and the pfx was sent by email to the user, the password for the pfx file will be stored in the "Last used pfx password" setting (see 13.4 for more information).

The user preference sub-pages "select encryption certificates", "select signing certificate", "templates" and "global preferences" will be explained in later paragraphs.

Security info		
Add security info	<input type="checkbox"/>	<input checked="" type="checkbox"/> inherit
Decrypted tag	<input type="text" value="[decrypted]"/>	<input checked="" type="checkbox"/> inherit
Signed tag	<input type="text" value="[signed]"/>	<input checked="" type="checkbox"/> inherit
Signed by tag	<input type="text" value="[signed by: %s]"/>	<input checked="" type="checkbox"/> inherit
Invalid signature tag	<input type="text" value="[invalid signature!]"/>	<input checked="" type="checkbox"/> inherit
Mixed content tag	<input type="text" value="[mixed content]"/>	<input checked="" type="checkbox"/> inherit
Subject filter		
Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/> inherit
Filter	<input type="text"/>	<input checked="" type="checkbox"/> inherit

Figure 21: Global advanced user preferences

5.2.13 Other

Server secret (R) The server secret is used to protect external resources against tampering (using the HMAC algorithm). 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. A global server secret will be automatically generated the first time the server starts. The server secret is a required setting. In most setups there is no need to override the inherited server secret.

Client secret (R) The “Client secret” is used to generate the one time password for the recipient.

Auto create client secret (R) If OTP mode is enabled and the recipient does not yet have a “Client secret” and “Auto create client secret” is enabled, a new randomly generated client secret will be automatically created for the recipient.

5.3 Global advanced settings

Certain settings can only be set for the global settings (see figure 21 for the global specific settings).

5.3.1 Security info

Add security info If checked and an incoming email is S/MIME encrypted or signed, information about the encryption or signature will be added to the subject. The actual text that will be added to the subject depends on whether the message is encrypted or signed and whether the signature is valid.

Decrypted tag If an incoming message is encrypted, the “Decrypted tag” will be added to the subject.

Signed tag If an incoming message is signed and the signature is valid, the “Signed tag” will be added to the subject.

Signed by tag If an incoming message is signed and the signature is valid but the email address of the sender (the from header) is not the same as the email address of the signing certificate, the “Signed by tag” will be added to the subject with %s replaced by the email address of the signing certificate.

Invalid signature tag If an incoming email is signed but the signature is not valid (for example the signing certificate is not trusted), the “Invalid signature tag” will be added to the subject.

Note: since an external sender can add these tags to an existing message (i.e., “spoof” that the message was protected), the existence of any of these security info tags should not be used as a proof that the message was encrypted and/or signed. Whether or not the message was really signed and/or encrypted can only be checked with 100% certainty by looking at the X-Djigzo-Info headers (see Appendix A of the Ciphermail S/MIME setup guide for more information on the X-Djigzo-Info headers). The “Subject filter” (see next section) can be used to remove all of the security info tags of incoming email to make sure that an external sender cannot “spoof” that the message was encrypted and/or signed.

5.3.2 Subject filter

Enabled (S & R) If checked, the subject of incoming email will be filtered.

Filter (S) The filter with which the subject will be filtered. The filter should be specified as:

/REG-EXP/ VALUE

where REG-EXP is the regular expression that will be used to match part of the subject and VALUE is the string that will replace the matched part. If VALUE is not set, the matched part will be removed from the subject (i.e., it will be replaced with an empty value)

Example: the following subject filter can be used to remove the default security info tags from incoming email:

```
/\[([decrypted|signed|signed by:.*|invalid signature!])\]/
```

5.4 Mobile

The mobile sub settings page contains settings which are only required when using “Ciphermail for BlackBerry”. See “Ciphermail for BlackBerry administration guide” for more information.

Note: The mobile settings page is disabled by default. If the BlackBerry add-in for BIS should be used, the mobile settings page should be enabled.

5.5 SMS

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

Send SMS (S) If checked, the sender of the message is allowed to send SMS Text messages.

Receive SMS (R) If checked, the recipient of the message is allowed to receive SMS Text messages.

Phone number allowed (S) If checked, senders are allowed to specify a telephone number on the subject of an outgoing message. This telephone number is used by the PDF encryption functionality to send passwords via SMS Text messages. The telephone number is only used when the subject trigger is specified (see “Subject trigger” on page 27) and when the telephone number is at the end of the subject line. The telephone number can start with a + and may contain spaces, and the following characters (excluding the quotes) “-()”.

Examples: Suppose that the subject trigger is [encrypt].

The following subjects contain valid telephone numbers:

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

(b) Encrypt this [encrypt] +31-(123)456

The following subjects do not contain valid telephone numbers:

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

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

It should be noted that only one recipient (“To”, “Cc” or “Bcc”) at the same time 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 (S) The telephone number in the subject should be in international format (i.e., including the country code). 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 when the telephone

Setting	Value	Inherit
Password		<input checked="" type="checkbox"/> inherit
Min. password strength	20	<input checked="" type="checkbox"/> inherit
Enabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> inherit
Auto invite	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> inherit
Base URL		<input checked="" type="checkbox"/> inherit

Figure 22: Portal settings

number is specified on the subject. The “Default country code” is not used by the telephone number that has been explicitly set using the administration page (see “Phone number” on page 40) since that number should always be set in international format.

5.6 Portal

The portal can be used to provide the following functionality for external users:

- PDF reply
- Manage a DLP quarantined message
- Generate the one time password

The portal settings page can be used to setup certain aspects of the portal (see figure 22).

Password The password is used by the external user to login to the portal. If an external user receives a PDF encrypted email which was encrypted with a one time password (OTP), the external user can login to the portal to retrieve the password for the PDF. If no password is set for the user, the user cannot login.

Min. password strength If the user sets or changes the portal password, the password should have a minimal strength. The password strength is estimated using the algorithm from “NIST Special Publication 800-63”. Before the new password is accepted, additional checks on the password strength are done. A new portal password is only accepted if the password:

1. is not based on your email address
2. does not contain a QWERTY keyboard sequence of more than 5 characters
3. does not contain more than 5 duplicate characters in a row
4. is of sufficient strength in bits

Note: The administrator is free to set any portal password for a user, i.e., there is not check on the strength of the password if set from the WEB GUI.

Enabled If set, the user can login to the portal using the email address of the user as the login name and the portal password for the user. If not set, the user cannot login.

Note: the enabled setting is only used to specify whether the user can login. If not set, users can still reply to a PDF since replying to a PDF does not require the user to login.

Auto invite If the “Auto invite” setting is set and a one time password encrypted PDF gets sent to the user, the user is “invited” to select a new password. See the PDF encryption guide for more information.

Base URL To access the portal functionality, external users need to connect to the portal. The URLs to which external users need to connect to are written to the emails and encrypted PDFs (for example the reply link in the PDF). To make sure the URLs are externally accessible URLs, the gateway has to know what the correct external URL of the portal is⁷. The “Base URL” is not directly used, but is used as the base for the following URLs: PDF reply URL, OTP URL and DLP Quarantine URL. The “Base URL” can only be set for the global settings.

Example: In most setups, the base URL should look similar to*:

```
https://www.example.com/web/portal
```

* replace `www.example.com` with the domain name or IP address of the real server.

Note: since all other URLs used by the gateway are based on the “Base URL”, it’s advised to only set the “Base URL” and not set the other URLs. The other URLs only need to be explicitly set if some specific functionality uses a different URL than the portal base URL.

5.7 PDF settings

only available with the enterprise edition

By clicking the PDF settings link on the settings page for a user, domain or global settings, the PDF settings page will be opened (see figure 23).

⁷In most typical setups, the gateways internal IP address is different from the external IP address (NAT).

PDF settings for global preferences

additional fonts

Cover page

Add cover page ☑ inherit

Cover page No file selected. (.pdf) ☑ inherit

Attachments

Auto rename attachments ☑ inherit

Attachments to rename ☑ inherit

Keyword to add to renamed attachments ☑ inherit

Portal

Max. attachment size (bytes) ☑ inherit

Max. number of attachments ☑ inherit

Other settings

Attach original message as RFC822 (.eml) ☑ inherit

Background color ☑ inherit

Figure 23: PDF settings

5.7.1 Cover page

The cover page ⁸ will be added to the beginning of the encrypted PDF. This can for example be used to add company logo and address information.

Add cover page If set and a cover page is set, the cover page will be added as the first page of the encrypted PDF.

Cover page The actual cover page. The cover page should be a valid PDF file with a maximum size of 1MB.

5.7.2 Attachments

Message attachments are added to the encrypted PDF as well. Some attachment types however are blocked by some PDF readers (for example Adobe Acrobat blocks access to zip files). The PDF encryption module can automatically rename attachment extensions so the PDF reader will not block access to the attachment ⁹.

Example: If a message is PDF encrypted and a zip file with name `a-file.zip` was attached to the message, the zip file will be renamed to `a-file.zip.RENAMED`.

⁸Although the cover page will be a single page in most setups, the PDF cover page can extend multiple pages

⁹The extracted attachment should be renamed by the recipient to the correct extension

Auto rename attachments If set, files that match a rule from the “Attachments to rename” list will be renamed by appending the keyword from the setting “Keyword to add to renamed attachments”.

Attachments to rename The list of filenames to rename. Multiple entries should be separated with space. Wildcard filename are supported.

Example: *.zip some-file.txt *.exe

5.7.3 Portal

Additional settings for the PDF reply portal page

Max. attachment size The maximum size (in bytes) of an attachment added to the PDF reply.

Max. number of attachments The maximum number of attachments allow to add to the PDF reply.

5.7.4 Other settings

Attach original message as RFC822 (.eml) If selected, the original message will be attached to the PDF. The eml file can be opened in the local email client. All message content, like HTML email will be intact. An additional benefit is that the recipient can store the message in unencrypted form.

Background color This allows the admin to change the background color of the PDF to match the color of the cover page.

5.8 Webmail

only available with the enterprise edition

Ciphermail Secure Webmail is a secure pull delivery webmail add-on to the Ciphermail encryption gateway. If the rules of the Ciphermail encryption gateway determine that a message must be encrypted, and S/MIME, PGP or PDF cannot be used, for example because there is no certificate for a recipient, the email will be sent to the Ciphermail Webmail box via an S/MIME secured tunnel. The recipient gets a notification that a new message is available. The first time the user receives a message, the user needs to select a secure password. The user can read and reply to the message using any web browser. This part only briefly explains the webmail settings for the gateway and how the gateway interacts with the webmail appliance. For more details on how to install and configure the webmail appliance, see the “Ciphermail Webmail Administration Guide” and “Ciphermail Webmail Quick Start Guide”.

The following steps are taken when sending an email to a recipient via secure webmail (see figure 24):

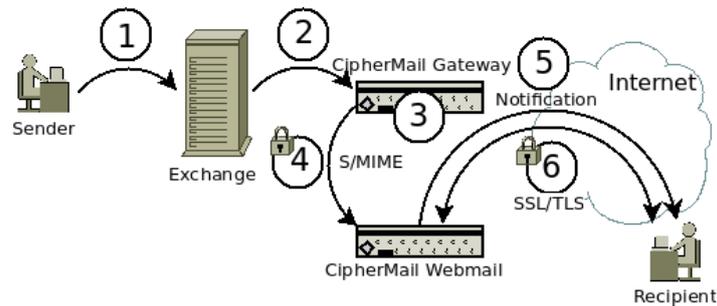


Figure 24: Webmail mail flow

1. User sends email via Exchange (or some other mail server)
2. Exchange forwards the message to the CipherMail gateway.
3. A rule on the CipherMail gateway flags that the email must be sent to webmail.
4. The message gets S/MIME signed with the webmail sender key and encrypted with the webmail recipient certificate and forwarded via email to the webmail appliance. The webmail appliance decrypts the mail, checks the signature and places the email in the mailbox of the recipient(s).
5. A notification message is sent to the recipient that a message is available for pick-up.
6. The user logs-in with a browser via HTTPS and reads the message.

5.8.1 Webmail settings

The webmail settings page (see figure 25) can be opened by clicking the “webmail” link on the settings page.

Enabled (S & R) If set, webmail will be enabled for the recipient.

Read receipt (S) If set, a read receipt header will be added to the message and a read receipt message will be sent when the recipient has opened the message. Alternatively, the sender can add a read receipt from the email client when sending the message. An example of a read receipt message:

This is a Return Receipt for your message

```
To: test <test@example.com>
Subject: demo webmail
Date: 2015-06-26 16:34
```

Note: This receipt only acknowledges that the message was displayed on the recipient's computer. There is no guarantee that the recipient has read or understood the message contents.

Webmail client settings for global preferences

create webmail certificate

User settings

Enabled	<input checked="" type="checkbox"/>		<input type="checkbox"/> inherit
Read receipt	<input type="checkbox"/>		<input checked="" type="checkbox"/> inherit
Only if mandatory	<input type="checkbox"/>		<input checked="" type="checkbox"/> inherit

Tunneling settings

Webmail recipient	<input type="text" value="webmail@webmail.local"/>		<input type="checkbox"/> inherit
Webmail sender	<input type="text" value="webmail@example.com"/>		<input type="checkbox"/> inherit

Figure 25: Webmail settings

Webmail recipient Email for the webmail appliance is routed to the webmail appliance via email. The “webmail recipient” is a specialized email address of the webmail appliance. The webmail appliance scans this email address for email from the gateway. The “webmail recipient” is a required setting otherwise the gateway is unable to route email to the webmail appliance.

Webmail sender Email for the webmail appliance needs to be S/MIME signed and is routed to the webmail appliance via email. The sender of the tunnel message, i.e., the message sent to the webmail appliance, is set to the “Webmail sender” address. The message is S/MIME signed with the key associated with the “Webmail sender” address.

5.8.2 Webmail tunnel certificate

Because email for the webmail appliance needs to be S/MIME signed, a valid signing certificate must be available. A valid S/MIME signing certificate and private key for the webmail S/MIME tunnel can be created by clicking the “create webmail certificate” link (see figure 25). On the “Create webmail tunnel certificate” page, the email address of the certificate is set to the “Webmail sender” address. Additional subject information can be specified before the certificate is created (see figure 26). The generated certificate will be a self signed certificate and automatically added to the certificate trust list.

Note: The “create webmail certificate” link is only available if the “Webmail sender” address is specified and applied.

Figure 26: Create webmail tunnel certificate

6 Domains

The domains page gives an overview of all the domains that have been explicitly added by the administrator (see figure 27). A domain can be used to setup preferences for all users of that domain. For example, a domain can be added to create 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 in that domain will be encrypted with the domain certificate. Normally a “virtual private network” (for example a TLS connection) is used for a secure tunnel between email servers. However, the problem with a VPN is that each intermediate email server must support encrypted connections and each intermediate server needs to be fully trusted (the email is stored unencrypted on the email server until forwarded to the next hop). When email is sent to domains which cannot be guaranteed to be secure (like for example Hotmail or Yahoo) use of an encrypted channel cannot be enforced. With S/MIME tunnelling, the message itself is encrypted and not just the connection. Because the message itself is protected, it can be sent over an unsecured connection.

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

7 Templates

Some actions require the gateway to send email or SMS Text messages. These messages are created from message templates which can be modified by the administrator¹⁰. The templates are MIME encoded messages. When modifying the templates, care should be taken that the templates are valid MIME messages. The following templates can be edited (see figure 28):

- encrypted PDF

¹⁰The templates are processed using the Freemarker template engine (see <http://freemarker.sourceforge.net>)

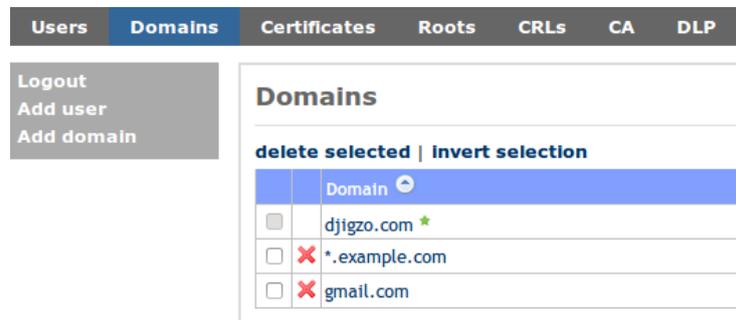


Figure 27: Domains

- Encrypted PDF via SMS
- Encrypted PDF OTP
- Encrypted PDF OTP invite
- Encryption failed notification
- Encryption notification
- Passwords notification
- SMS with password
- BlackBerry S/MIME
- SMS PFX password
- PFX email
- DLP warning
- DLP quarantine
- DLP block
- DLP error
- DLP release notification
- DLP delete notification
- DLP expire notification

Note: The “SMS PFX password” and “PFX email” templates can only be edited for the global settings.

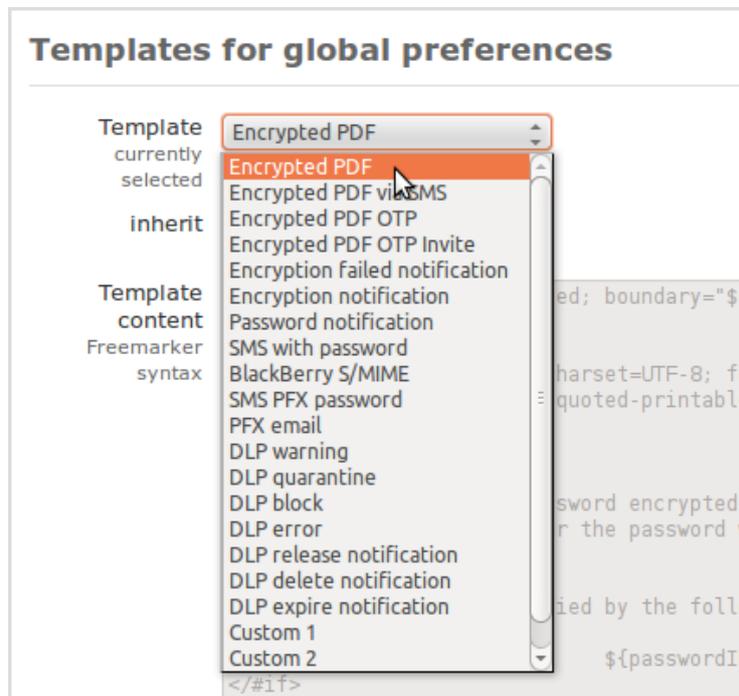


Figure 28: Message templates

encrypted PDF The template for the final message of an encrypted PDF message. When a message is PDF encrypted the actual message content, including the attachments, is converted to an encrypted PDF. This encrypted PDF is then attached to a message and the message, with the encrypted PDF, is sent to the final recipient. The PDF attachment in the template is just a “dummy” PDF which will be replaced by the real encrypted PDF. This template is used when the PDF password was not newly generated (i.e., the PDF password was a static password or was still valid).

Encrypted PDF via SMS This template is similar to the “encrypted PDF” template. The only difference is that this template is used when the PDF password is newly generated and the password was sent via an SMS Text message to the recipient.

Encrypted PDF OTP This template is similar to the “encrypted PDF” template. The only difference is that this template is used when the PDF password is generated using the one time password (OTP) functionality.

Encrypted PDF OTP invite This template is similar to the “Encrypted PDF OTP” template. The only difference is that this template is used when the recipient does not yet have a password set.

Encryption failed notification Template used for the notification message that the message could not be encrypted but encryption was mandatory.

Encryption notification Template used for the notification message that the message was successfully encrypted. This template is only used when the sender of the message has “Encryption notification” enabled (see page 24).

Passwords notification Template used for the notification message containing newly generated passwords (see “Send to originator” on page 27 for more info).

SMS with password Template for the SMS Text message containing the generated password. The complete SMS Text message should fit in one SMS Text message (maximum 160 characters). The template should therefore not be too large.

BlackBerry S/MIME Template used for the S/MIME email message when the recipient preference “Recipient uses add-on” is enabled. Any S/MIME message sent to a recipient having “Recipient uses add-on” enabled, is converted to a message that can be read on a BlackBerry using the “Ciphemail for BlackBerry” add-on. See “Ciphemail for BlackBerry administration guide” for more information.

SMS PFX password Template for the SMS Text message containing the password for the encrypted private key file. The complete SMS Text message should fit in one SMS Text message (maximum 160 characters). The template should therefore not be too large. For more information see the CA section 13. Note that this template can only be edited for the global settings.

PFX email Template for the email containing the password protected private key file (.pfx). For more information see the CA section 13. Note that this template can only be edited for the global settings.

DLP templates For more information about the DLP specific templates, see the separate “DLP setup guide”.

8 Certificates

Ciphemail gateway supports S/MIME for encryption and digital signing of email messages. S/MIME is based on PKI and X.509 certificates¹¹. The system has a built in X.509 certificate store. Certificates can be manually added and removed by the administrator. Certificates attached to incoming digitally signed messages are automatically extracted from the signature and are added to the

¹¹For more information on S/MIME and X.509 see <http://en.wikipedia.org/wiki/SMIME> and <http://en.wikipedia.org/wiki/X.509>

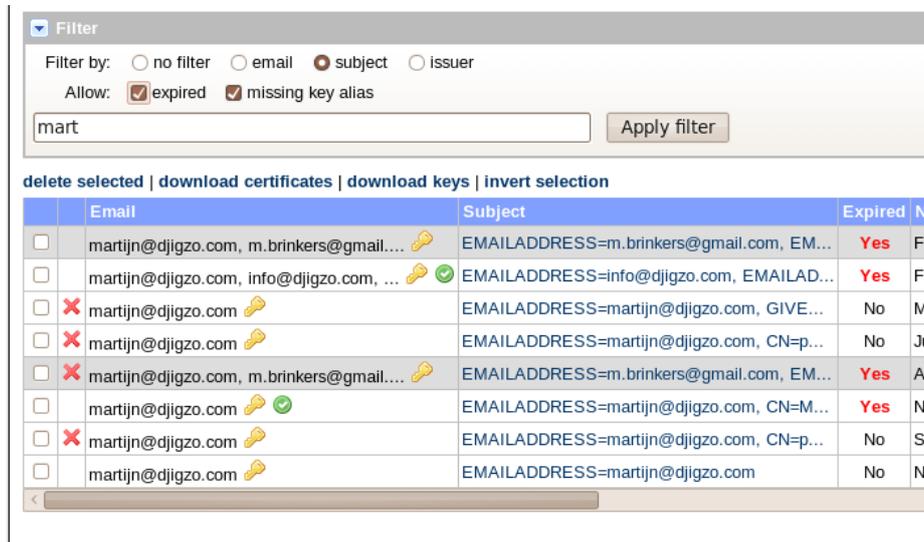


Figure 29: Certificate store

“Certificates” store. The certificate store supports unlimited number of certificates¹². Intermediate and end-entity certificates are stored in the “Certificates” store and root certificates are stored in the “Roots” certificate store. The Certificates page shows all the certificates in the “Certificates” store (see figure 29).

Specific certificates can be searched with the certificate filter. Certificates which are not valid (not signed by a trusted root, revoked, expired etc.) are shown in gray. Certificates with an associated private key contain the “key” icon. Certificates which are revoked are shown in red.

Ciphermail gateway follows RFC 3280 (“Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List 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”).

Certificate details can be opened by clicking on the certificate subject (see figure 30). By clicking the “usage” sub-menu it is shown which users or domains are using the certificate. The certificate details page can be used to get more info as to why a certificate is not valid. For example, figure 30 shows 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 the X.509 certificate. Private keys can be used for decrypting S/MIME encrypted messages or for digital signing of messages. An entry with an associated private key has a non-empty “Key alias” (see for example figure 30). By unchecking the “allow missing key alias” checkbox only certificates for which there is a private key available will be shown.

¹²Limited 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](#) | [usage](#) | [add to CTL](#)

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
Path Length Constraint:
Subject Key Identifier:
Thumbprint (SHA-512): 731747A73AE08DBE2E87C84ADC81BF1D9FE739C6E67CCDC391BDB2AB25A4FCAC4A6A3C0AA82738C7218687184D7D1
Signature Algorithm: SHA1WITHRSA
Public Key Length: 1024
Public Key Algorithm: RSA
CRL distribution points:
Key Alias: 731747A73AE08DBE2E87C84ADC81BF1D9FE739C6E67CCDC391BDB2AB25A4FCAC4A6A3C0AA82738C7218687184D7D1
Private Key Available: true
Private Key Accessible: true
Inherited: false
CTL Status:
Info: Error building certPath. Certificate has a critical 'extended key usage' but EMAILPROTECTION parameter is missing.

Figure 30: Certificate details

The “Roots” store contains certificates which are fully trusted by the administrator (i.e., trust is explicit and not inferred from other certificates). The “Roots” store normally only contains certificates (i.e., the “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 are stored in the certificates store. Most S/MIME signed messages contain at least the signing certificate.

The certificate can be added to the “Certificate Trust List” by clicking “add to CTL”. “Certificate Trust List” will be explained in section 12.

8.1 Importing Certificates

Certificates can be imported into a store with the “Import certificates” page (see figure 31). A certificate file, a store to import to and additional import parameters should be selected. 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. After the import the “Import certificates” page will show how many certificates were imported.

8.2 Importing keys

Certificates with associated private keys can be imported into the “Certificates” store using the “Import keys” page (see figure 32). A password protected “PKCS#12” private key file (.p12 or .pfx) must be selected and uploaded.

The screenshot shows a web interface with a top navigation bar containing 'Users', 'Domains', 'Certificates', 'Roots', 'CRLs', 'CA', 'DLP', and 'Settings'. The 'Certificates' tab is active. On the left, there is a sidebar with 'Logout' and 'Add user' links. The main content area is titled 'Import certificates' and contains the following elements:

- A text box: "On this page, certificates can be imported. In most cases, import Multiple certificates can be imported at the same time from a pe"
- A 'Certificate file' input field with a 'Browse...' button. Below it, the text reads: "public key file (.cer/.p7b)".
- A 'Store' dropdown menu with 'Certificates' selected. Below it, the text reads: "store to import to".
- 'Import checks' section with two options: skip self-signed and must be self-signed. Below it, the text reads: "certificate requirements".
- 'Expired' section with skip. Below it, the text reads: "skip expired certificates".
- 'Import' and 'Cancel' buttons at the bottom.

Figure 31: Certificate import

The screenshot shows a web interface with a top navigation bar containing 'Users', 'Domains', 'Certificates', 'Roots', 'CRLs', 'CA', 'DLP', and 'Settings'. The 'Certificates' tab is active. On the left, there is a sidebar with 'Logout' and 'Add user' links. The main content area is titled 'Import Private Keys' and contains the following elements:

- A text box: "On this page, private keys and their associated certificates can b S/MIME signing of outgoing email and for the decryption of incon"
- A 'Private key file' input field with a 'Browse...' button. Below it, the text reads: "private key file (.pfx/.p12)".
- A 'Password' input field. Below it, the text reads: "private key file password".
- 'Missing private key' section with skip. Below it, the text reads: "skip certificate only entries".
- 'Import' and 'Cancel' buttons at the bottom.

Figure 32: Key import

8.3 Download certificates and keys

Certificates and associated private keys can be downloaded from the gateway. Select the certificates that need to be downloaded and click “download certificates” or “download keys” from the sub-menu. When downloading private keys, a password used for encrypting the private key file (.p12 file) must be entered.

9 S/MIME

In this section a brief introduction of S/MIME will be given. S/MIME is based on “Public Key Infrastructure” (PKI) and uses X.509 certificates.

9.1 PKI

Public Key Infrastructure is a technology which can be used to securely exchange information over insecure networks using public key cryptography. PKI uses X.509 certificates to bind a public key to an identity. The main advantage of PKI is that there is no need to directly trust everyone involved because trust can be inferred. Roughly speaking there are two trust models in use today: hierarchical (via trusted CAs) or “Web Of Trust”.

With the hierarchical trust model, trust is inferred bottom-up. The root (the bottom) is blindly trusted (that makes it by definition a root) and all leaf nodes and branches (the end-user and intermediate certificates) are trusted because they are child’s of the trusted root (to be precise the intermediate certificates are issued by the root certificate). S/MIME uses a hierarchical trust model.

In a “Web of Trust” model, trust is inferred from trusted neighbours in a mesh like structure (a web). **For example:** “Alice” trusts “Bob” and “Ted” trusts “Alice” and therefore “Ted” now also trusts “Bob” (through “Alice”). The hierarchical model can be viewed as a “Web of Trust” model with additional constraints.

Because trust is inferred from other entities, it is possible to securely check whether one entity trusts another entity and that it is not possible to “spoof” any trust. Trust checking is done using “Public Key Cryptography”. An intermediate certificate is digitally signed by the issuer of the certificate using the issuers private key. With the public key of the issuer, it can be checked whether the certificate was really issued by the issuer. The public key together with some extra information forms an X.509 certificate.

9.2 X.509 certificate

A typical X.509 certificate contains the following elements (this is a non-exhaustive list):

- Public Key
- Subject
- Email address
- Issuer

- Serial Number
- Not Before
- Not After
- Key Usage
- Extended Key Usage

An X.509 certificate is digitally signed by the issuer of the certificate. By digitally signing the certificate, any changes done after signing will break the signature. Any changes to the certificate will therefore be noticed. A brief introduction of some of the main elements of an X.509 now follows.

Public Key The public key, like the name already implies, is the key that everyone is allowed to know. If a message must be encrypted, the public key of the recipient is used for encryption. The public key is used to verify a digital signature (the digital signature is created with the associated private key).

Subject The subject of a certificate contains the name of the “owner” and optionally an email address (or sometimes multiple email addresses).

Email address A certificate can contain multiple email addresses. X.509 certificates for S/MIME should normally contain the email address for which the certificate was issued.

Issuer The issuer contains the name of the issuer of this certificate (i.e., the issuer element should be equal to the subject of the issuer). If the subject of a certificate is equal to the issuer of a certificate the certificate is most likely a self-signed certificate. Root certificates are almost always self-signed.

Serial Number Every certificate should have a serial number. The serial number should be unique for the issuer (i.e., an issuer should use the serial number only once).

Not Before This is the date at which the certificate becomes valid. If the current date is before the “Not Before” date, the certificate is not yet valid.

Not After This is the date at which the certificate is no longer valid. If the current date is after the “Not After” date, the certificate is no longer valid.

Key Usage The public key of the certificate can be used for multiple purposes. Sometimes however the issuer of the certificate wants to restrict the key usage to only certain types. The following key usage types can be identified:

- digitalSignature

- nonRepudiation
- keyEncipherment
- dataEncipherment
- keyAgreement
- keyCertSign
- CRLSign
- encipherOnly
- decipherOnly

If the key usage is not specified it implies that the key may be used for all purposes. For S/MIME encryption, if a key usage is specified it should at least contain “keyEncipherment”. For S/MIME signing, if a key usage is specified it should at least contain “digitalSignature” or “nonRepudiation”.

Extended Key Usage The extended key usage, if specified, further specifies for what purposes the certificate has been issued. The following extended key usages can be identified:

- anyKeyUsage
- serverAuth
- clientAuth
- codeSigning
- emailProtection
- timeStamping
- OCSPSigning
- IPSecEndSystem
- IPSecUser
- IPSecTunnel
- smartcardLogin

If the extended key usage is not specified it implies that the key may be used for all purposes. For S/MIME, if an extended key usage is specified, it should at least contain “anyKeyUsage” or “emailProtection”.

Thumbprint The thumbprint is strictly speaking not part of an X.509 certificate. The thumbprint is the “cryptographic hash”¹³ calculated over the bytes of the encoded certificate. The thumbprint uniquely identifies a certificate. The default algorithm used by the Ciphermail gateway for calculating the thumbprint is “SHA-512”.

¹³See http://en.wikipedia.org/wiki/Cryptographic_hash_function for more info on cryptographic hash functions.

9.3 Revocation checking

Sometimes it can happen that a certificate should no longer be used. For example because the “private key” has been compromised or an employee has left the company. Certificates can be revoked by putting the certificates on a “Certificate Revocation List” (CRL). A CRL is issued by a certificate authority (CA) and is periodically updated. A revoked certificate should no longer be used. When a CRL is not available or when the administrator would like to “black list” a specific certificate, the certificate can be added to the “Certificate Trust List” (CTL). For more info on CTL see section 12.

10 Certificate selection

When required the Ciphermail gateway will automatically select the correct certificates for signing and encryption. Only certificates that are valid (i.e., trusted, not expired, not revoked) are automatically used. This implies that certificates should be trusted by a root certificate. The root certificate store by default does not contain any certificates¹⁴. The administrator should therefore add all the root certificates trusted by the organization to the root store. If a root certificate is not available a certificate can be “white listed” by adding the certificate to the “Certificate Trust List”.

10.1 Encryption certificate selection

Encryption certificates can be selected for a user, a domain or for 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 18). The “select encryption certificates” page shows all the certificates that have been selected for the user (or domain or global settings). When the certificate selection page has been opened, by default, only certificates with matching email addresses will be shown (see figure 33).

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. The certificate will only be automatically selected when the email addresses match. If a certificate is not automatically selected (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 33 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 the private keys associated with one the public keys used for encryption. The main advantage of using all of the selected certificates is that it allows the recipient to use different keys for decryption. For example, the key stored on the recipients home computer can be used when the message is read at home and the key on the office computer can be used when the message is read at the office.

¹⁴A collection of some well known CA certificates can be downloaded from the Ciphermail website.

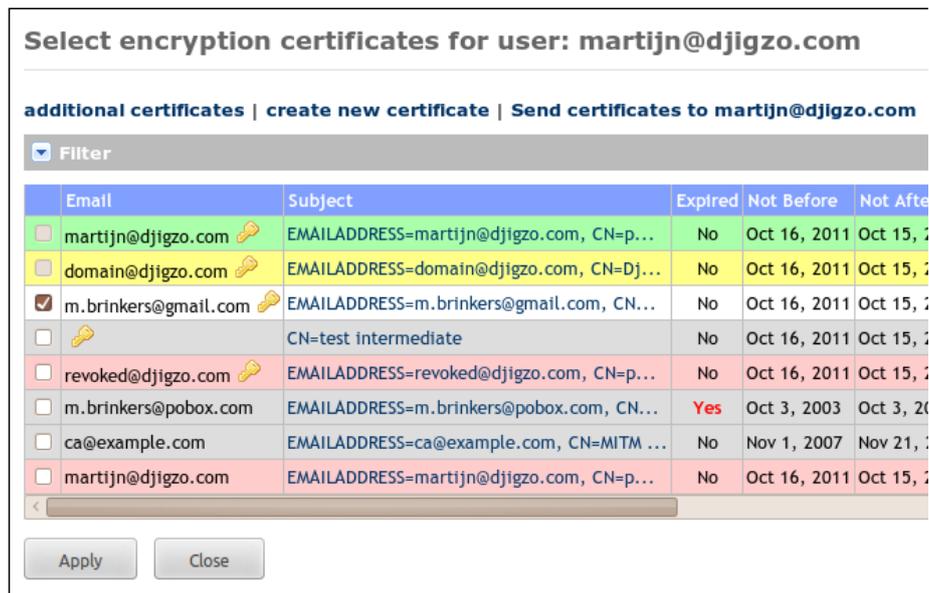


Figure 33: Select encryption certificates

The sender does not know at which location the recipient will open the email so it's better to encrypt the message with both certificates.

Color coding The selected certificates are color coded based on validity and inheritance of the certificates (see figure 34):

Valid Auto select Inherited Invalid Revoked

Figure 34: Color coding

Certificates can be manually selected and deselected by selecting the certificate checkbox and applying the settings. Automatically selected certificates cannot be deselected (the certificate can be completely removed if the certificate is no longer required). Uncheck "Auto select certificates" for the user if automatic selection of certificates for the user is not required.

Even when a certificate is manually selected it does not automatically mean that the certificate will be used for encryption. If a certificate is not valid it's not used for encryption. For example figure 33 shows that two certificates are manually selected. One certificate is however not valid ("gray color") because it has expired. This certificate is therefore not used when a message is encrypted for this user. If a manually selected but invalid certificate must be used, the certificate must be made valid (add for example the certificate to the CTL to make it valid).

Besides selecting certificates, the "Select encryption certificates" page supports the creation of new end-user certificates for external users with the built-in CA server. A certificate can also be securely transported via email to an exter-

Select signing certificate for user: martijn@djigzo.com

[back to user settings](#) | [create new certificate](#)

Filter

Filter by: no filter email subject issuer

Allow: expired missing key alias

auto select certificate

	Email	Subject	Expired	Not Before	Not Af
<input checked="" type="radio"/>	martijn@djigzo.com	EMAILADDRESS=martijn@djigzo.com, CN=p...	No	Feb 20, 2011	Feb 20
<input type="radio"/>	martijn@djigzo.com	EMAILADDRESS=martijn@djigzo.com, CN=p...	No	Feb 20, 2011	Feb 20
<input type="radio"/>	martijn@djigzo.com	EMAILADDRESS=martijn@djigzo.com, CN=p...	No	Feb 20, 2011	Feb 20

Figure 35: Select signing certificate

nal end-user. For more information on the built-in CA functionality see section [13](#).

10.2 Signing certificate selection

A signing certificate can be selected for a user, a domain or for 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 [18](#)). The “select signing certificate” page shows the signing certificate that has been selected for the user (or domain or global settings). When the certificate selection page has been opened, only certificates with matching email addresses will be shown by default (see figure [35](#)). Only certificates with an associated private key can be selected and only one signing certificate per user can be selected at the same time. The system tries to automatically select a signing certificate by searching for a valid certificate with a matching email address. If there are multiple certificates suitable for signing, the first certificate found will be selected. The administrator can override the automatically selected certificate by manually selecting another certificate. If a certificate was manually selected the selected certificate can be reverted back to an automatically selected certificate by pressing “auto select certificate”.

10.3 Additional certificates

If a message is S/MIME encrypted, the message can also be encrypted with additional certificates. For example, a company policy might dictate that all encrypted data should be readable even when the sender and or recipient no longer have access to the private key (key escrow). Another reason to encrypt the data with an additional encryption certificate is that it allows a centralized

CRLs

delete selected | download selected | invert selection | update CRL store

1 2 3

	Issuer	This Update	Next Update	Version	CRL Num
<input checked="" type="checkbox"/>	✗ CN=UTN - DATACorp SGC, OU=http://www.usertrust....	Jan 12, 2009	Jan 16, 2009	2	687
<input type="checkbox"/>	✗ CN=Serasa Certificate Authority II, OU=Serasa C...	Jan 12, 2009	Jan 12, 2009	2	BE57
<input type="checkbox"/>	✗ CN=Serasa Certificate Authority III, OU=Serasa ...	Jan 12, 2009	Jan 12, 2009	2	BE5A
<input type="checkbox"/>	✗ CN=Serasa Certificate Authority I, OU=Serasa CA...	Jan 12, 2009	Jan 12, 2009	2	BE5B
<input type="checkbox"/>	✗ CN=Equifax Secure eBusiness CA-1, O=Equifax Sec...	Jan 12, 2009	Jan 22, 2009	1	
<input type="checkbox"/>	✗ CN=UTN-USERFirst-Hardware, OU=http://www.usertr...	Jan 12, 2009	Jan 16, 2009	2	6EA
<input type="checkbox"/>	✗ CN=TDC OCES CA, O=TDC, C=DK	Jan 12, 2009	Jan 13, 2009	2	3EABB
<input type="checkbox"/>	✗ CN=UTN-USERFirst-Object, OU=http://www.usertrus...	Jan 12, 2009	Jan 16, 2009	2	697

Figure 36: CRL store

virus scanner to scan the email. Additional certificates can be selected using the “additional certificates” sub-menu (see figure 33). Additional certificates are inherited just like regular encryption certificates and can be selected for the global settings, the domain settings or for a user.

Note: Anyone with access to the private key of the additional certificate(s) can in principle decrypt all encrypted email. The private keys of the additional certificates should therefore be stored in a safe place and only be used when required.

11 Certificate Revocation List

A certificate revocation list (CRL) is a list of certificates¹⁵ which have been revoked and which should therefore no longer be used. Certificates can contain “CRL distribution points”. A “CRL distribution point” contains URLs from which the latest CRL can be downloaded. Periodically all the URLs from all the “CRL distribution points” for all the trusted certificates¹⁶ are collected and the latest CRLs are then downloaded from these URLs¹⁷. The downloaded CRLs are stored in the CRL store (see figure 36).

CRL details can be viewed by clicking the CRL “Issuer” link (see figure 37). CRLs which are not valid (incorrectly signed, no path to a trusted root etc.) are shown in gray. The details page provides more information on why a CRL is not valid. By default the CRL store is periodically updated every 12 hours. A CRL update can be forced by clicking “update CRL store” in the sub-menu. The CRL entries (the serial numbers of the revoked certificates and optionally a revocation reason) can be downloaded as a text file by clicking “download CRL entries” (see figure 37).

¹⁵to be precise it's actually a list of serial numbers issued by the CA

¹⁶by default, CRLs will only be downloaded from valid certificates

¹⁷CRL distribution over HTTP(s) and LDAP is supported.

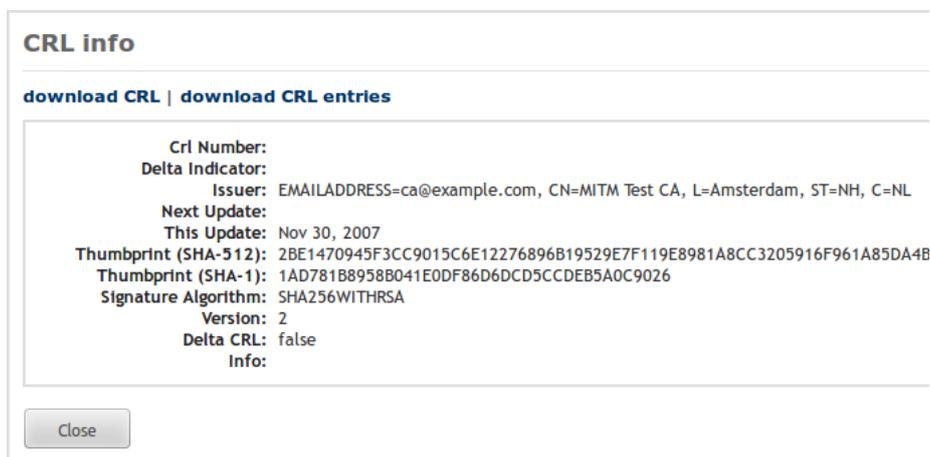


Figure 37: CRL details

Note: Some CRLs contain an extremely large number of revoked certificates. Downloading the entries of these large CRLs is therefore not advised.

12 Certificate Trust List

A Certificate Trust List (CTL) is a list of certificates (to be precise, a list of certificate thumbprints) which are explicitly trusted (“white listed”) or explicitly distrusted (“black listed”). The administrator can manually add or remove certificates to the Certificate Trust List.

In most cases PKI is sufficient for deciding whether or not a certificate is valid. Sometimes however, the administrator needs more control over this automatic process. Some examples when a CTL can be helpful:

- (a) A certificate should no longer be used because it was compromised but the certificate issuer does not have a CRL. In this case the administrator can “black list” the certificate.
- (b) A certificate is not valid because the root is missing. The administrator however knows that the certificate is valid (for example the thumbprint has been checked over the phone). After “white listing” the certificate the administrator can manually select the certificate for a user.
- (c) A certificate is not valid because the certificate has expired. However, the administrator is 100% certain that the certificate is still ‘valid’. By “white listing” the certificate and checking the “Allow expired” checkbox the certificate can now be manually selected.

By clicking “Certificate Trust List” on the left hand side menu of the certificates page (see figure 38) the “Certificate Trust List” can be opened. The “Certificate Trust List” contains the thumbprints of all the certificates that have been added to the CTL (see figure 39). A new entry can be added to the CTL by clicking

The screenshot shows a web interface for managing certificates. The top navigation bar includes 'Users', 'Domains', 'Certificates' (selected), 'Roots', 'CRLs', 'CA', 'DLP', and 'Settings'. A left sidebar contains 'Logout', 'Add user', 'Import certificates', 'Import keys', and 'Trust List'. The main content area is titled 'Intermediate and user certificates' and features a 'Filter' checkbox, action links for 'delete selected', 'download certificates', 'download keys', and 'in', and a table of certificates.

	Email	Subject
<input type="checkbox"/>	ca@example.com	EMAILADDRESS=ca@example.com, CN=
<input type="checkbox"/>	test@example.com	EMAILADDRESS=test@example.com, CN=
<input type="checkbox"/>	info@djigzo.com	EMAILADDRESS=info@djigzo.com, CN=p
<input type="checkbox"/>	m.brinkers@pobox.com	EMAILADDRESS=m.brinkers@pobox.com

Figure 38: Open Certificate Trust List

The screenshot shows the 'Certificate Trust List' interface. It includes a 'delete selected' and 'invert selection' link, and a table with columns for 'Status', 'Allow Expired', and 'Thumbprint'.

	Status	Allow Expired	Thumbprint
<input type="checkbox"/>	Whitelisted	false	2F461CC6DAD0446244E2524C
<input type="checkbox"/>	Blacklisted	false	72E92205F5BE2E36AC07BEE/

Figure 39: Certificate Trust List

“Add CTL entry” on the left hand side menu. A CTL entry does not directly contain a certificate, it contains the thumbprint of a certificate. The reason for this is that it should be possible to “white list” or “black list” a certificate even if the certificate is not available in the certificate store. An expired certificate can be made valid by by checking “Allow expired”. “Allow expired” is only applicable when “white listing” a certificate.

Trust inheritance “Black listing” a certificate is inherited by certificates issued by that certificate. This means that if an intermediate certificate is “black listed” all certificates, directly or indirectly, issued by that intermediate certificate are also “black listed”. “White listing” is not inherited. If an intermediate certificate is “white listed”, certificates issued by that intermediate certificate are not automatically “white listed”. For a certificate to be “white listed” it has to be explicitly added to the “Certificate Trust List”.

Example: Suppose a trusted root has issued multiple intermediate certificates. Normally all the intermediate certificates issued by that root are trusted. The administrator however does not trust one of the intermediate certificates. Removing the root from the root store won’t help because the result would be that none of intermediate certificates are trusted. By “black listing” one of the intermediate certificates all certificates issued by that intermediate certificate

will also be (implicitly) “black listed”.



Figure 40: Certificate Trust List Icons

CTL icons When a certificate is “white listed” or “black listed” an icon is added next to the email address of the certificate (see figure 41). The green icon is shown when the certificate is “white listed” and the yellow icon is shown when the certificate is “black listed” (see figure 40). Clicking one of the icons will open the CTL entry page for the certificate.

Final note: the “Certificate Trust List” should normally only be used as a “work around” for when the standard PKI rules are not sufficient. Using the “Certificate Trust List” to manage trust is much more time consuming than managing trust using PKI.

13 Certificate Authority (CA)

The gateway contains a built-in CA server which can be used to create end-user certificates for internal and external users. This helps to quickly setup an S/MIME infrastructure without having to resort to external CAs for certificates and keys. Certificates and private keys can be securely transported to external recipients using a password encrypted certificate store (.pfx). The external recipients can use the certificate with any S/MIME capable email client like “Outlook”, “Outlook express”, “Lotus Notes” and start receiving and sending S/MIME encrypted email without having to install additional software.

The Ciphermail gateway contains a pluggable framework which allows new certificate request handlers to be registered. A certificate request handler is

	Email	Subject
<input type="checkbox"/>		CN=DOD EMAIL CA-12, OU=PKI, OU=DoD, O...
<input type="checkbox"/>		CN=test intermediate
<input type="checkbox"/>	domain@djigzo.com	EMAILADDRESS=domain@djigzo.com, CN=pe...
<input type="checkbox"/>	martijn@djigzo.com	EMAILADDRESS=martijn@djigzo.com, CN=p...
<input type="checkbox"/>	martijn@djigzo.com	EMAILADDRESS=martijn@djigzo.com, CN=p...

Figure 41: “white listed” and “black listed” certificates

responsible for creating and/or retrieving a certificate and private key from internal or external CAs. By default, there are currently three certificate request handlers available: “built-in”, “delayed built-in” and “EJBCA”.

A brief explanation of the CA functionality will now follow. For a more thorough overview on how to setup the S/MIME infrastructure see the separate “S/MIME setup guide”.

Note: the built-in CA has limited functionality. If support for multiple CA profiles, OCSP, CRLs for intermediate and root certificates is required a dedicated external CA should be used instead (for example EJBCA).

13.1 Create new CA

Before starting to create end-user certificates, a root and intermediate certificate should be created¹⁸. The “Create new CA” page (see figure 42) can be used to create a new CA (i.e., create a new intermediate and root certificate).

Some details about the root and intermediate certificates should be specified before the certificates can be created (see figure 42).

Validity The number of days the root or intermediate certificate is valid (starting from the day it was created). This is a mandatory property.

Key length The length of the public key in bits (1024, 2048 and 4096). A 2048 bits key is sufficient in most cases. This is a mandatory property.

Email The email address that will be added to the certificate. Leave it empty (unless your policy requires an email address for your CA).

Common name The “common name” of the certificate is the main identifier of the certificate. The common name of the root certificate must be different from the common name of the intermediate certificate. Choose a unique common name and do not reuse a common name.

More Selecting “more” enables the following advanced settings for the subject: “organization”, “first name” and “last name”. These settings are only used to make it easier for end users to identify the CA certificates.

Make default CA If checked, the newly created CA will be the default CA.

Signature algorithm The algorithm used for signing the root and intermediate certificate. Windows versions prior to “XP-sp3” do not support “SHA256 With RSA” or better. If older Windows versions should be supported you are advised to use “SHA1 With RSA”. If support for older Windows versions is not required you are advised to select “SHA256 With RSA”.

¹⁸If a root and intermediate certificate is already available import them into the certificate and root store.

Certificates Roots CRLs **CA** DLP Settings Queues

Create new CA

The built-in Certificate Request Handler requires a root and intermediate certificate.

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: Sha1 With Rsa

Create Cancel

Figure 42: Create new CA

CA settings

Default end-user certificate settings

Common name

Validity in days

Key length in bits

Signature algorithm for certificate signature

CA email

Password length in bytes

Store password

Add CRL dist. point

CRL dist. point fully qualified URL

Certificate Authority the CA to use for the certificate request

Apply Cancel

Figure 43: CA settings

13.2 CA settings

When the “Create new end-user certificate” page is opened the default dialog values are taken from the “CA settings”. The “CA settings” can be opened from the CA settings sub-menu (see figure 43). The settings “Common name”, “Validity”, “Key length” and “Signature algorithm” were already explained (see page 64)

CA email The sender email address used when sending certificates to end-users by email. Make sure that the CA email address is a valid email address. Because the email containing the encrypted certificate is sent by the gateway, the settings for the CA email user should be such that the email is not encrypted by the gateway (i.e., set encrypt mode of the CA user to “No Encryption”). If a certificate and key must be sent to an external recipient the CA email address

must be set.

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

Password length The certificate creation page can automatically generate a password for the encrypted private key container (.pfx). The number of random bytes used to generate the password is set with the password length.

Store password This will be the default value for "Store password" for the "Create new end-user certificate" page. If checked the password for the last generated pfx file for a user will be stored in the "Last used pfx password" preferences of the user (see [5.2.12](#)).

Add CRL dist. Point This is the default value for "Add CRL dist. Point" for 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 newly generated end-user certificate.

CRL dist. Point The CRL distribution point added to the end-user certificate. The CRL distribution point is only added if "Add CRL dist. Point" is set. This is the default value for the "CRL distribution point" setting for the "Create new end-user certificate" page.

Certificate Authority The default CA used when a certificate is requested. The default "Certificate Authority" is for example used when a certificate is automatic requested for a sender when the sender does not yet have a valid signing certificate and "Auto request certificate" is enabled for the sender. See section [13.3](#) for more information on "Certificate Request Handlers" and Certificate Authorities.

13.3 Certificate Request Handlers

A certificate request handler is responsible for creating and/or retrieving a certificate and private key from internal or external CAs. The Ciphermail gateway contains a pluggable framework which allows new certificate request handlers to be registered. By default, there are currently three certificate request handlers available: "built-in", "delayed built-in" and "EJBCA".

Some certificate request handlers should be setup before they can be used. Certificate request handlers can register a configuration page which can be used to setup the certificate request handler. The available certificate request handler configuration pages can be accessed using the "Request handlers" left-hand side menu on the "CA" page. The "Registered Certificate Request Handler configuration pages" page shows all registered certificate request handler configuration pages (see figure [44](#)).



Figure 44: Registered Certificate Request Handler configuration pages

13.3.1 built-in certificate request handler

The built-in certificate request handler uses the built-in CA for creating new certificates. Certificates created with the built-in certificate request handler will be issued by the default selected CA (see section 13.5 for more information on selecting the default CA). The built-in certificate request handler creates a private key and certificate instantly without any delay (i.e., a request for a certificate is synchronously handled).

13.3.2 delayed built-in certificate request handler

The delayed built-in certificate request handler is similar to the built-in certificate request handler. The only difference is that with the delayed certificate request handler, the request will be handled asynchronously by the background request handler thread.

If “Auto request certificate” (see page 30) is enabled and message throughput should not be impacted when a new certificate is requested, it’s better to use the delayed built-in certificate request handler because all certificate requests will then be handled asynchronously. If however a certificate should be used immediately when requested, the built-in certificate request handler should be used.

13.4 Create new end-user certificate

With the CA page a new end-user certificate can be created (see figure 45). Before an end-user certificate can be created a CA should be available. A warning will be shown if no CA is available or if a default CA is not selected. The general and Certificate subject settings have already been discussed.

Email delivery The email delivery settings are required when the newly created certificate and private key should be securely sent to an external recipient. If the “Send by email” checkbox is checked a password used for the protection of the certificate and private key should be set.

A password can be randomly generated by pressing the “gear” icon on the right hand side of the password edit field. If a password is manually set 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 send

13.4 Create new end-user certificate 13 CERTIFICATE AUTHORITY (CA)

Create new end-user certificate

On this page, a certificate and private key for an end-user can be created. The ce

[create CRL](#) | [send certificates](#) | [bulk request](#) | [pending requests](#)

General

validity in days

Key length in bits

Signature algorithm for certificate signature

Certificate subject

Email required

Common name required

more

Email delivery

Send by email
send key file to user

Password
password for key file

SMS password
send password via SMS

Store password
store the pfx password in the user preferences

Advanced

show advanced settings

Add CRL dist. point
add to certificate

CRL dist. point
fully qualified URL

Certificate Authority
the CA to use for the certificate request

Add user
add a user object for the requested certificate

Figure 45: Create end-user certificate

The default CA will be the default CA used for issuing end-user certificates.

Email	Subject	Expired	Not Before	Not After
<input checked="" type="radio"/>	CN=test intermediate	No	Apr 18, 2013	Apr 18, 20...
<input type="radio"/> ca@example.com	EMAILADDRESS=ca@example.com, CN=MITM ...	No	Nov 1, 2007	Nov 21, 20...

Select Cancel

Figure 46: Select default CA

it by regular post or give the password in person. Alternatively the gateway can send the password via an SMS Text message.

SMS password If the “SMS password” checkbox is checked the password for the protected certificate and private key file will be sent to the recipient via an SMS Text message. This requires that the SMS gateway is correctly setup (see section 17) and that the recipients telephone number is added to the user settings of the recipient.

Store password If checked the password for the last generated pfx file for a user will be stored in the “Last used pfx password” preferences of the user (see 5.2.12).

Advanced settings With the advanced settings page the CRL distribution point for the certificate can be specified. A CRL distribution point should be a fully qualified URL pointing to the location where the latest CRL for the CA can be downloaded. If a CRL for the CA should be created and published make sure that the correct URL is specified. 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 only if all the settings are valid, a new end-user certificate is created. If “Send by email” was checked the certificate and key will be password protected with the password and sent to the recipient by email. If “SMS password” was checked the password will be sent via an SMS Text message to the recipients telephone number. For a more thorough explanation of this procedure see the “S/MIME administration guide”.

13.5 Select default CA

There can be multiple CAs but only one can be active at the same time. Select the default CA with the “Select default CA” page (see figure 46).

Pending certificate requests

Email filter

delete selected | reschedule selected | invert selection

	ID	Email	Subject	Iteration	Info
<input type="checkbox"/>	247	test0@example.com	EMAILADDRESS=test0@example.com, GIVEN...	0	
<input type="checkbox"/>	248	test1@example.com	EMAILADDRESS=test1@example.com, GIVEN...	0	
<input type="checkbox"/>	249	test2@example.com	EMAILADDRESS=test2@example.com, GIVEN...	0	
<input type="checkbox"/>	250	test3@example.com	EMAILADDRESS=test3@example.com, GIVEN...	0	

Figure 47: Pending certificate requests

13.6 Pending requests

Some certificate request handlers do not immediately issue a certificate (i.e., the certificate is asynchronously issued). For example the Comodo certificate request process requires several steps (see appendix F for more information). Certificate requests which are not immediately handled are stored in the “pending requests” store and handled asynchronously by a background thread (see figure 47).

13.7 Bulk request

With the bulk request option, multiple certificate requests can be issued at the same time. A comma separated text file containing the request details can be uploaded (see figure 48). The certificates will be requested using the selected certificate request handler. To make sure that the request details are correctly imported, a preview of the imported certificate requests will be shown after pressing “Request preview” (see figure 49). See appendix G for details of the comma separated file format.

Note: Certificate requests for email addresses for which there already is a valid signing certificate, will be skipped.

13.8 Create CRL

Sometimes a certificate should no longer be used even when it is not yet expired. A certificate revocation list (CRL) is used to revoke a specific certificate issued by a CA. With the “Create CRL” page a CRL for the internal CAs can be created or updated. Before the CRL can be created the CA, which will issue the CRL, must be selected (see figure 50).

After selecting the CA the “Create CRL” page is opened on which the certificates that should be revoked can be added to the list of revoked certificates. A brief explanation of the dialog fields:

Serial numbers A certificate issued by a CA is uniquely identified by the serial number. The serial numbers list contains all the serial numbers that are about to be revoked.

Bulk request new end-user certificate

On this page, multiple certificates can be requested by uploading a comm format)

Import settings

Request file
csv file with all requests

Validity
in days

Key length
in bits

Signature algorithm
for certificate signature

Advanced

show advanced settings

Figure 48: Bulk request

Certificate requests preview

The following certificates will be requested*. Please verify the request details before starting the request procedure.
 * if there is already a valid signing certificate for a user, the request will be skipped.

Email filter

delete selected | invert selection

	Email	Subject	Validity	Key Length	Certificate F
<input type="checkbox"/>	test0@example.com	EMAILADDRESS=test0@example.com, GIVEN...	365	2048	delayed built
<input type="checkbox"/>	test1@example.com	EMAILADDRESS=test1@example.com, GIVEN...	365	2048	delayed built
<input type="checkbox"/>	test2@example.com	EMAILADDRESS=test2@example.com, GIVEN...	365	2048	delayed built
<input type="checkbox"/>	test3@example.com	EMAILADDRESS=test3@example.com, GIVEN...	365	2048	delayed built

Figure 49: Certificate request preview

Create CRL

A certificate on a CRL is identified by the serial number of the certificate.

Create a CRL for CA certificate: **EMAILADDRESS=ca@example.com, CN=I**

Serial numbers
serial numbers of revoked certificates

Revoked certificate
serial number in hex. form

Next update
in days

Update existing CRL
add to existing CRL

Signature algorithm
for CRL signature

Figure 50: Create CRL

Revoked certificate Add a new certificate to the list of certificates to be revoked by entering 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 CRL¹⁹. If the CA contains a CRL distribution point (see section 13.1) make sure that a new CRL is available and download-able from the CRL distribution point before the CRL expires. 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. 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. It’s best to always update an existing CRL because certificates that are previously revoked should remain revoked.

Signature algorithm The CRL will be signed by the issuing CA. A CRL should be signed to make it possible for external parties to check whether the CRL is a valid CRL and is issued the CA. Windows versions prior to “XP-sp3” do not support “SHA256 With RSA” or better. If older Windows versions should be supported you are advised to use “SHA1 With RSA”. If support for older Windows versions is not required you are advised to select “SHA256 With RSA”.

Clicking the “Create CRL” button will create the new CRL. The new CRL will be automatically added to the CRL store (see section 11). If the CA specifies a CRL distribution point the CRL should be published. Download the CRL from the CRL store and upload it to the CRL distribution point URL.

13.9 Send certificates

Sometimes end-users require a copy of their certificates (and private keys). For example they experienced a system crash and had to completely reinstall the system (and forgot to make a backup).

The “Send certificates” page can be used to send a new copy of the certificate and private key to an external user. This is also known as “key escrow”. Clicking “Send certificates” opens the “Send selected certificates to recipient” page (see figure 51). Sending CA certificates by email is not allowed. This is done to prevent accidental leakage of CA certificates.

Password This has already been explained. See section 13.4.

SMS password This has already been explained. See section 13.4.

¹⁹The 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.

Send selected certificates to recipient

With the send certificates page, certificates and the associated private keys can be sent to an attached to a newly generated email. The email is then sent to the recipient. The recipient can

Selected certificates

Filter

Filter by: no filter email subject issuer

Allow: expired missing key alias

	Email	Subject	Expired	Not Before	Not After
<input type="checkbox"/>	ca@example.com	EMAILADDRESS=ca@example.com, CN=MITM ...	No	Nov 1, 2007	Nov 21, 20...
<input type="checkbox"/>	test@example.com	EMAILADDRESS=test@example.com, CN=Val...	No	Nov 1, 2007	Nov 21, 20...
<input type="checkbox"/>	info@djigzo.com	EMAILADDRESS=info@djigzo.com, CN=pers...	No	Apr 18, 2013	Apr 18, 20...
<input type="checkbox"/>		CN=test intermediate	No	Apr 18, 2013	Apr 18, 20...

Delivery details

Email
email address of recipient

Password
password for the certificate

SMS password
send password via SMS

Store password
store the pfx password in the user preferences

Allow mismatch
allow mismatch between certificate email and recipient

Figure 51: Send selected certificates to recipient

	ID	Key ID	Email	User IDs	Expiration
<input type="checkbox"/>	24	D80D1572D0486F55	test@example.com	test multiple sub keys (test multiple...	
<input type="checkbox"/>	44	4EC4E8813E11A9A0	test@example.com	test key djigzo (this is a test key) ...	
<input type="checkbox"/>	47	4605970C271AD23B	martijn@djigzo.com	Martijn Brinkers <martijn@djigzo.com>	Oct 2, 20...
<input type="checkbox"/>	51	94CEE89F0C345BCC	info@djigzo.com	DJIGZO <info@djigzo.com>	

Figure 52: PGP keyring

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

Allow mismatch By default, email addresses in the certificate must match the email address of the recipient. However, there are situations where the certificate and private key should be sent to a different email address. By checking “Allow mismatch” the certificates and keys can be sent to non matching email addresses. The “Allow mismatch” check is added to prevent any leakage of certificate(s) and key(s) because of an accidental mistype of the recipients email address.

14 OpenPGP

OpenPGP is an email encryption and digital signing standard which is similar to S/MIME. OpenPGP works with public and secret keys. Public keys can be signed by other public keys (although in practise most keys are only self-signed). PGP public keys can be published to public accessible key servers. Public keys can be downloaded from public key servers if a public key is not yet locally available for a recipient.

OpenPGP supports two forms of encoding: PGP/MIME and PGP/INLINE. With PGP/MIME the MIME message (HTML parts and attachments) is signed and/or encrypted as a whole. With PGP/INLINE, every part of the message is individually signed and/or encrypted. Since PGP/MIME keeps the structure of the original message intact and supports HTML, PGP/MIME is strongly advised. The PGP keyring stores all the public and secret keys (see figure 52). Keys with an associated private key are shown with a yellow key symbol next to the Key ID.

14.1 Importing keys

Secret and public key rings can be imported from a file by clicking “Import keyring” on the left hand side menu (see figure 52). On the import key ring

Import keyring

On this page, public and secret keyrings can be imported into the keyring. Importing a s

Keyring keyring file No file selected.

Password
Only required when importing a secret keyring

Figure 53: Import PGP key ring

page the key ring file and a password (if importing a secret key ring) should be specified (see figure 53).

14.2 Creating keys

A new secret key ring can be created by clicking “Create keyring” on the left-hand side menu. On the PGP key ring page, the email address which will be used for the User ID, the name and the key size of the generated keys can be specified (see figure 54). If “Publish key” is selected, the generated key ring will be automatically published to the registered key servers. The generated secret key ring will be added to the key ring and automatically trusted.

14.3 Search keys

With the “Search keys” page, a search can be done for a key on the registered key servers. The search keys page can be opened by clicking “Search keys” on the left-hand side menu. The keys returned from the search can be downloaded and imported into the key ring by selecting the keys and then selecting “import selected” (see figure 55). Imported keys are not automatically trusted unless the checkbox “Automatically trust imported key” is selected.

Note: searching for key ID or fingerprint requires that the search query is prefixed with 0x. For example, to search for a key with key ID 271AD23B, the search query should be 0x271AD23B.

14.4 Key servers

The list of registered key servers can be managed by clicking “Key servers”. Key servers can be added or removed (see figure 56).

Create new secret keyring

Create a new secret keyring for an email address. A master key and encryption sub key will be created.

Email
email part of the User ID

Name
name part of the User ID

Key size
in bits

Publish key
automatic publish the key to the key servers

Create Close

Figure 54: Create PGP secret key ring

Search keys

Search for PGP keys on the registered key servers. Only new keys, i.e., keys which are not yet in the key ring, will be imported.

Note: If searching on Key ID or fingerprint, prefix the search query with 0x (example: to search for a key with Key ID 271AD23B, use the search query 0x271AD23B)

Search query

Exact matches only

Import settings

Automatically trust imported key

Import selected | Invert selection

Key ID	User IDs	Algorithm	Key Length	Creation Date	Expiration Date	Flags	Key server URL
<input type="checkbox"/> AF29335EE9DA5BEC89883CACB9167144A3C41EB	<martijn@djigzo.com>	RSA	2048	Mar 10, 2014		r	http://pool.sks-ke
<input type="checkbox"/> DC368B248911C140EF6564764605970C271AD23B	Martijn Brinkers <martijn@djigzo.com>	RSA	2048	Oct 3, 2013	Oct 2, 2018		http://pool.sks-ke
<input type="checkbox"/> 0BCF54328534C59DC8363D7D94CEE89F0C345BCC	DJIGZO <info@djigzo.com>	DSA	1024	May 17, 2012			http://pool.sks-ke

Close

Figure 55: Search PGP keys

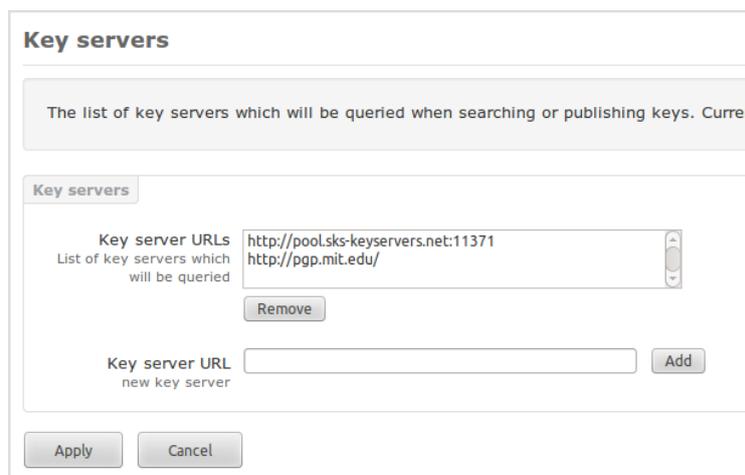


Figure 56: PGP key servers

Note: currently only key servers that support the OpenPGP HTTP Keyserver Protocol (HKP) are supported.

14.5 Key details

The details page of a key can be opened by clicking the Key ID of the key. The key details page shows the most relevant key parameters. If the key is a master key and the key contains sub keys, all the sub keys will be shown below the key details (see figure 57). The details of a sub key can be shown by clicking the Key ID of the sub key.

14.6 Key trust

A key by default is not trusted. The trust level of a key can be managed by clicking “key trust”.

14.7 Publish public key

The public key (including the sub keys) can be published to the registered key servers by clicking “publish public key”.

Note: the public key option is only available for a master key.

14.8 Email addresses

Before a key can be used, it has to be associated with an email address. When a key gets imported, it is automatically associated with the email address extracted from the User IDs. Quite often however the email address from the User ID is outdated. Either because the email address is no longer used or the

Details for key with ID 4EC4E8813E11A9A0

[key trust](#) | [publish public key](#) | [email addresses](#) | [revoke key](#)

Details

ID: 56
 User IDs: [test key djigzo (this is a test key) <test@example.com>]
 Email: [test@example.com]
 Key ID: 4EC4E8813E11A9A0
 Parent Key ID:
 Creation Date: Oct 9, 2013
 Expiration Date:
 Insertion Date: Feb 13, 2014
 Private Key Available: true
 Valid For Encryption: false
 Valid For Signing: true
 Fingerprint: F372FCF8208776062C69C1854EC4E8813E11A9A0
 Sha256 Fingerprint: ADE29F0A314B1760C151946F4E6F8E97B251B464DDE17003DA44DE07C3B20995
 Key Length: 2048
 Master Key: true
 Parent ID:
 Valid: true
 Failure Message:

Sub keys

[delete selected](#) | [invert selection](#) | 25

	ID	Key ID	Email	User IDs	Expiration Date	Encrypt	Sign	Key Length	Fingerprint
<input type="checkbox"/>	58	8AAA6718AADEAF7F				true	false	2048	1F73FAF306

Figure 57: PGP key details

owner of the PGP key is using a new email address. By clicking the “Email address” sub menu on the key details page (see figure 57), the email addresses associated with the key can be managed. Associated email addresses can be added or removed (see figure 58).

14.8.1 domains

In addition to email addresses, a domain can also be associated with a key. This makes it possible to use the key as a domain key (i.e., encrypt all email to the domain with the domain PGP key).

Note: email addresses can only be associated with a master key.

14.9 Revoke key

A key for which there is a private key can be revoked. A revoked key can no longer be used. After revoking a key it's advised to (re) publish the key to the key servers.

14.10 Key selection

When sending email the gateway will automatically select the keys for encryption and signing. Whether or not a key is used for encryption and/or signing

Manage associated address of the PGP key with key ID D

This page shows the email addresses that are associated with this public key. New e

Email addresses and domains

Addresses
email addresses and domains associated with the key

test@example.com

Remove

Address
email address or domain to add to the list

Add

Apply Cancel

Figure 58: Associated email addresses

depends on a number of factors. The requirements for encryption keys are different then the requirements for signing keys.

14.10.1 Email encryption key

A key will be used for encryption if the following key requirements are met:

1. The key must be trusted
2. The key must not be expired
3. The key must not be revoked
4. The email recipient must match an associated email address or domain of the key
5. The key must be valid for encryption

The encryption key will be automatically selected for every recipient. To check which keys are selected for a recipient a search for the email address (or domain) can be executed on the PGP keyring page. Another way to check which key is selected for a recipient or domain is by adding a user or domain and selecting “encryption keys” of the PGP pulldown menu on the user or domains settings page (see figure 59). The selected encryption keys for the recipient (or recipients domain if a domain was selected) will be shown on PGP encryption key page (see figure 60). If there are multiple valid keys available for a recipient, the email will be encrypted with multiple keys.

14.10.2 Email signing key

A key will be used for digital signing if the following key requirements are met:

1. A private key is available



Figure 59: PGP encryption keys menu

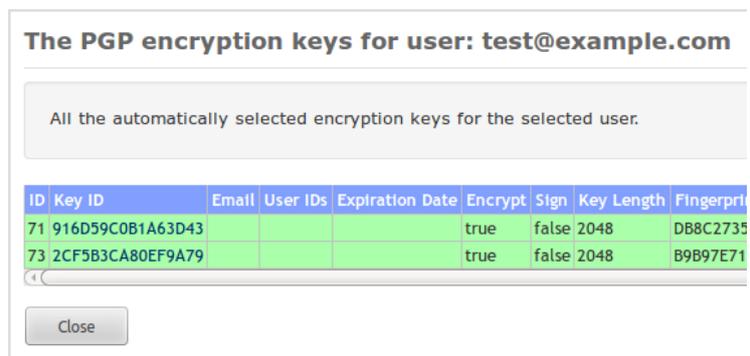


Figure 60: PGP encryption keys

2. The key must be trusted
3. The key must not be expired
4. The key must not be revoked
5. The from sender address must match an associated email address or domain of the key
6. The key must be valid for signing

The signing key will be automatically selected for a sender. To check which signing key is selected, add a user or domain and select “Signing key” of the PGP pulldown menu on the user or domains settings page (see figure 61). The selected signing key for the sender (or senders domain if a domain was selected) will be shown on PGP signing key page (see figure 62). Only the selected signing key will be used for signing. If there are multiple keys which can be used for signing are available, a new signing key can be set by selecting the signing key and applying the settings.

15 PDF encryption

The problem with S/MIME is that it requires the recipient to use an S/MIME capable email client²⁰ and the recipient must have a certificate and a private key.

²⁰Most email clients however support S/MIME out of the box

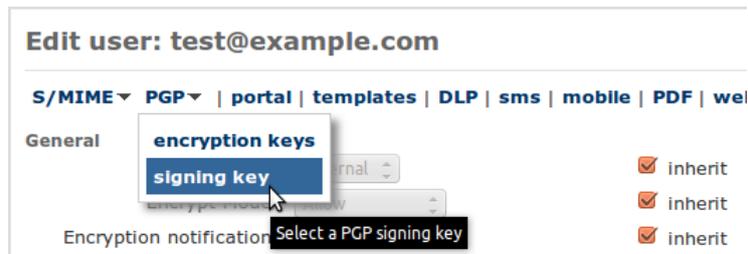


Figure 61: PGP signing key menu

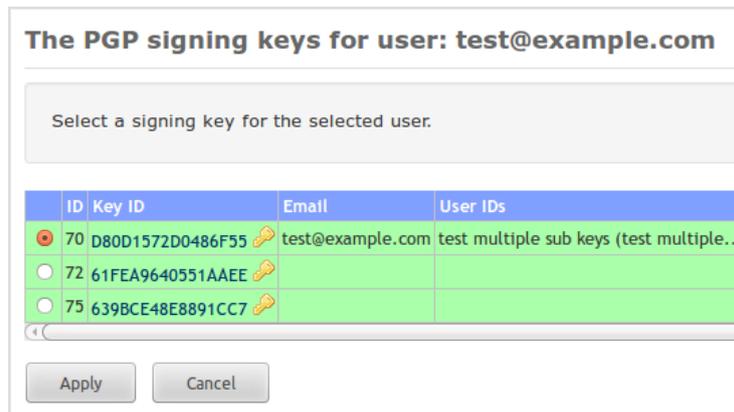


Figure 62: PGP signing keys

Although installing a certificate and a private key is not hard, even less so when using the gateways built-in CA functionality, it may still be too cumbersome for some recipients. Especially when only a few secure email messages need to be exchanged over a longer period.

As an alternative to S/MIME encryption, PDF encryption can be used. The PDF standard allows a PDF to be encrypted with a password²¹. Files can be added to the PDF and are encrypted as well. Because most recipients already have a PDF reader installed they do not need to install or configure any software.

When the gateway PDF encrypts a message it converts the complete email message, including all attachments, to a PDF. The PDF is then password encrypted and attached to a new message (which is based on a template). This message does not contain any information other than a general note that the message contains an encrypted PDF (see section 7 for the templates). There are different options on how to password encrypt the PDF:

- (a) The PDF can be encrypted using a pre-defined static password.
- (b) The PDF can be encrypted using randomly generated password. The password will then be sent by SMS Text to the recipient.
- (c) The PDF can be encrypted using randomly generated password. The password will be sent back to the sender of the message.
- (d) The PDF can be encrypted using a one time password (OTP) algorithm.

The four password options will be briefly explained. For more details see the PDF encryption guide.

Static password To use a pre-defined and static password for PDF encryption, the password for the recipient should be set. To make sure that the password will always be valid (i.e., that it will never expire), either set the “Validity interval” to -1 or make sure that the “Date set” password setting is not set.

Send password by SMS Text If setup correctly, the system can automatically send the generated password to the recipient via an SMS Text message. This requires that the SMS “Phone number” is set for the recipient. Alternatively, if the user is allowed to add a telephone number to the subject (see page 40), the mobile number can be specified on the subject of the email. Figure 63 shows the complete PDF encryption process when using the SMS option.

Send to originator If the “Send to originator” option is enabled, the generated password(s) will be sent back to the sender of the message. The sender is then responsible for securely delivering the passwords to the recipients.

One time password (OTP) If the one time password option is enabled, the PDF password will be generated using a one time password algorithm. The recipient can login to the portal to retrieve the PDF password.

²¹The PDF is encrypted with AES128 with a key based on the password.

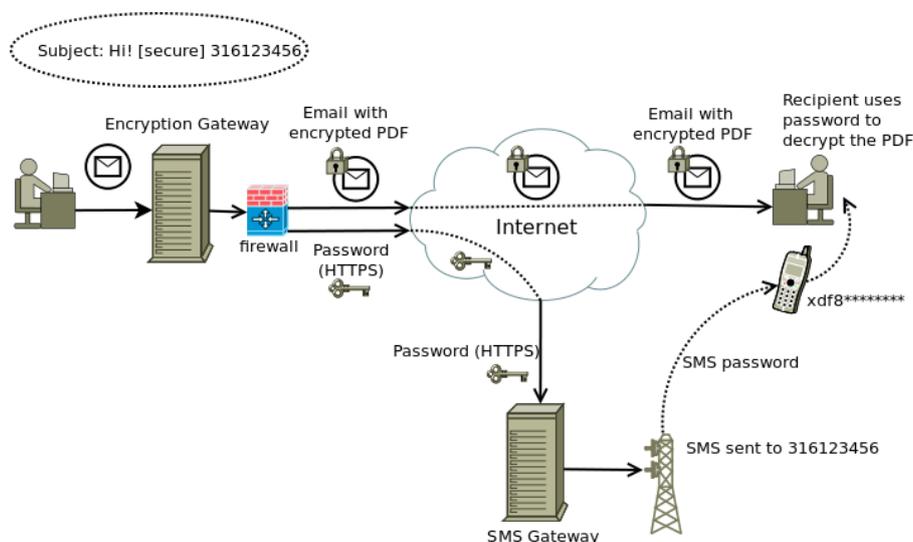


Figure 63: PDF encryption

15.1 Encrypted PDF message

The recipient receives a message with a standard message (based on a template) with the encrypted PDF attached (see figure 64 for an example opened in Gmail). When the PDF is opened, the PDF reader asks for the password (see figure 65). Only after entering the correct password will the PDF content be shown. The PDF is formatted to make it look like a normal email message. The attachments can be accessed from the attachment pane at the bottom (see figure 66).

15.2 Replying

A recipient can reply to the encrypted PDF message by clicking the “Reply” link (see figure 64). An on-line portal, via a secure “HTTPS” connection, will be opened (see figure 67). The reply URL in the PDF is equal to the “Reply URL” parameter at the time the encrypted PDF was created (see paragraph 5.2.4). The user can now enter a message body and add attachments (by default maximum 3). The reply will be sent via the Ciphermail gateway. Because the reply is sent via the Ciphermail gateway it can be encrypted as well (see “Reply Sender” at page 34).

16 DLP

Data Leak Prevention (DLP) is a feature that prevents certain information to leave the organization via email. What information this is, is defined in the configuration of the DLP system. Typically, it includes credit card numbers, bank account numbers, excessive amounts of email addresses or other personal information in one email message, etc. DLP is implemented as a filter on out-



Figure 64: PDF encrypted message

going email.

DLP can monitor email at various levels:

- email body content
- email headers
- email attachments of various types
- nested attachments of various types

The Ciphermail DLP engine currently only filters email bodies, attachments and nested attachments of type text, html, xml and other text-based formats. Filtering attachments of type pdf, doc, xls etc. will be part of a future offering of the Ciphermail DLP engine. For more information about setting up the DLP functionality, see the separate “DLP setup guide”.



Figure 65: PDF encrypted message

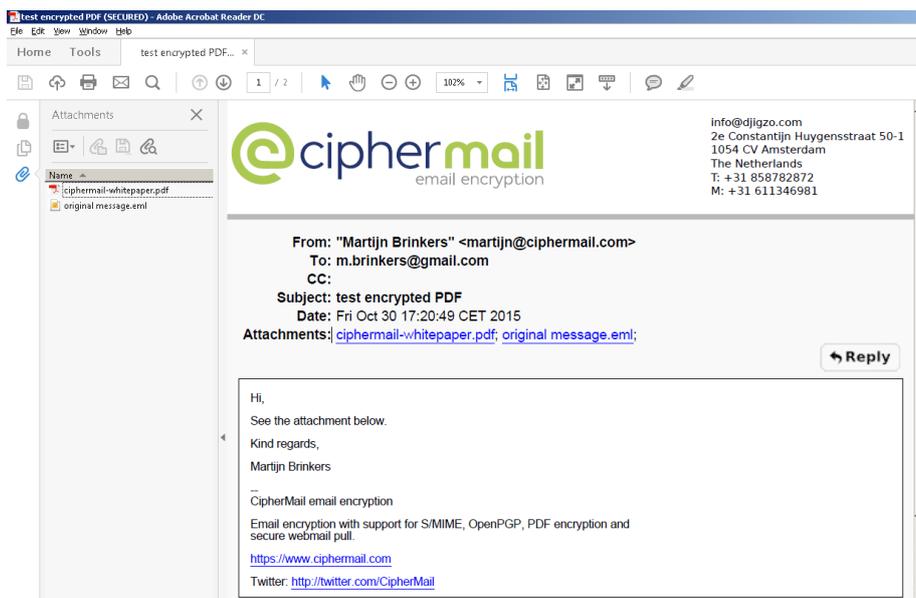


Figure 66: PDF decrypted

17 SMS gateway

The Ciphermail gateway contains an SMS gateway which can be used for sending generated passwords via SMS Text messages. The SMS gateway can use different SMS transports for the delivery of SMS Text messages²². The default SMS transport is set to Clickatell (see <http://www.clickatell.com> for more information). SMS Text messages are sent via a secure HTTPS connection to Clickatell. When an SMS Text message is sent, it is queued for delivery until the message has been delivered with the active SMS transport (see figure 68). To test the SMS gateway an SMS Text message can be manually added with “Add SMS”.

17.1 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

²²Currently only Clickatell and Gnokii (direct connection to Nokia phones) are supported.

Compose a reply message en ▾

From: m.brinkers@gmail.com
 To: test@example.com
 Subject: Re: test

Attachment No file selected.
max. size 5 MB

aanvraag_indelingsverzoek_iud0361z1folre.pdf ✖

Reply (max 100000 characters)

See my answer in the attached document

Kind regards,
 Martijn Brinkers

Figure 67: PDF reply

SMS queue Queue

MTA | MPA outgoing | MPA error | MPA spool | MPA respool | DLP quarantine | SMS

delete selected | invert selection | send SMS

	ID	Phone Number ↕	Created ↕
<input type="checkbox"/>	✖ 91	123456	04/19/2013 18:07

Figure 68: SMS gateway

Figure 69: Clickatell settings

HTTPS connection). A Clickatell account must be created and configured before any SMS Text messages can be sent. See <http://www.clickatell.com> for more information about the sign-up process.

During the sign up process a HTTP connection must be added ²³ (leave the “Callback” parameters empty). The connection has an associated “API ID” which is required for the Clickatell transport. Open the Clickatell transport configuration page by opening the “SMS” page and clicking the “Clickatell settings” left-hand side sub-menu (see figure 69). The first three settings: “API id”, “User” and “Password” are mandatory. The “From” parameter can be set to the sender of the SMS Text message (i.e., the telephone number of the sender) but only after the telephone number has been approved by Clickatell.

Clickatell uses pre-paid message credits. To check how many credits are left (and for testing the login credentials), click “update balance”.

Note: newly entered transport settings are only used after the changes have been applied. Before clicking “Update balance”, make sure all changes are applied.

18 Mail Queues

Postfix is used as the MTA for sending and receiving of email to internal and external recipients. Internally a Java based SMTP server is used for message processing (the “Mail Processing Agent”). The MTA and MPA store all mail into different mail queues.

²³See the Clickatell “HTTP API Specification v.2.x.x” document for more information

Certificates Roots CRLs CA DLP Settings Queues Logs Admin							
Mail transfer agent Queue							
MTA MPA outgoing MPA error MPA spool MPA respool DLP quarantine SMS							
Filter							
delete selected hold selected release selected requeue selected flush invert selection 25							
	Queue ID	status	size	Arrival Time	Sender	Recipients	Failure
<input checked="" type="checkbox"/>	4993F3FC1E	Deferred	588947	Fri Apr 19 17:52:02	martijn@djigzo.com	test@example.com	(connect to 192.168.1.2[192.

Figure 70: Mail Queues

The mail queues of the MTA and MPA can be viewed and managed using the “Queues” page (see figure 70). There are five different mail queues: “MTA”, “MPA outgoing”, “MPA error”, “MPA spool” and “MPA respool”.

MTA queue With the MTA queue page messages on the MTA queue can be removed, put on hold, viewed etc.

MPA queues The MPA contains four queues: “MPA outgoing”, “MPA error”, “MPA spool” and “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.

19 Logging

The “Logs” page is used to view the MTA and MPA logs. A keyword filter can be set to view only a subset of all the log entries (see figure 71). The search keyword is highlighted in yellow. Every email is tagged with a unique “Mail ID” (shown in a green color). This makes it easier to track an email while the email is being processed. Color coding of certain log elements is used to make it easier to spot certain details (for example an email address is shown in a blue color, an error in red).

20 Administrators

Multiple administrators, each with a different set of roles, can be registered. The “Admin” page shows a list of all the registered administrators (see figure 72). A new administrator can be added by clicking “Add admin” on the left-hand side menu. This will open the “Adding new administrator” page (see figure 73).

20.1 Roles

An administrator can have any of the following roles:

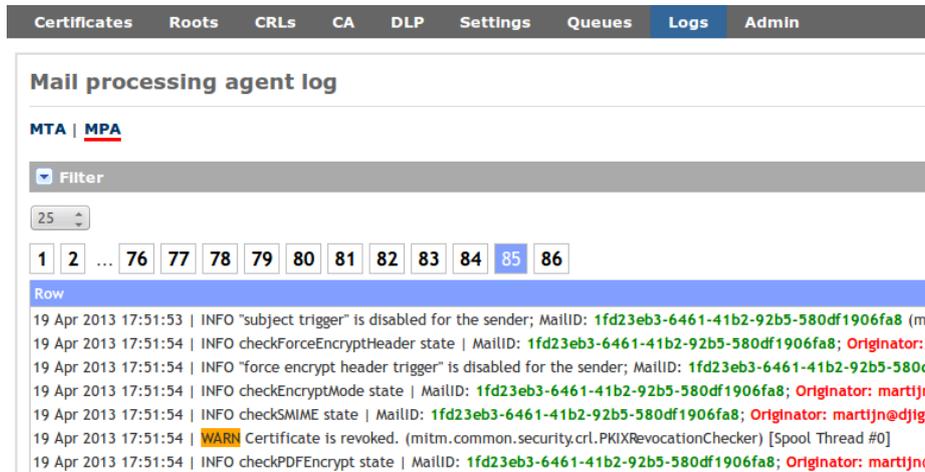


Figure 71: Logging

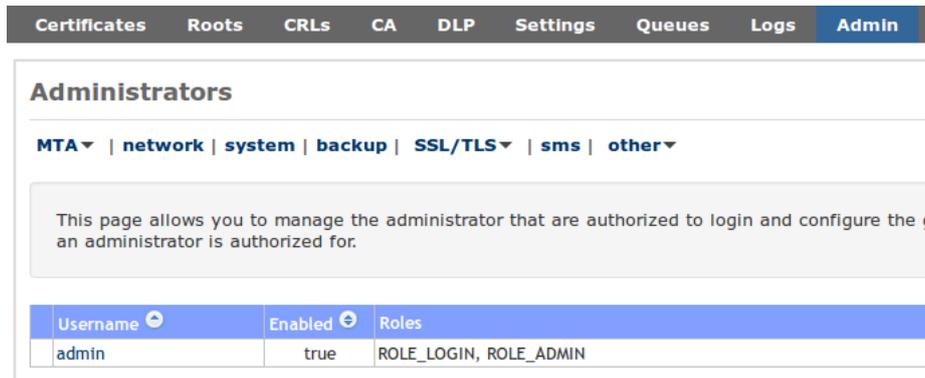


Figure 72: Administrators

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

Adding new administrator

Name

Password
min. size 6 chars

Password
repeat password

Roles
select roles

Available	Selected
ROLE_ADMIN	ROLE_LOGIN
ROLE_DLP_MANAGER	
ROLE_DOMAIN_MANAGER	
ROLE_GLOBAL_MANAGER	
ROLE_LOG_MANAGER	
ROLE_MOBILE_MANAGER	
ROLE_PDF_MANAGER	
ROLE_PKI_MANAGER	
ROLE_PORTAL_MANAGER	
ROLE_QUARANTINE_MANAGER	

Add Cancel

Figure 73: Add new administrator

- ROLE_DLP_MANAGER
- ROLE_QUARANTINE_MANAGER
- ROLE_MOBILE_MANAGER
- ROLE_PORTAL_MANAGER

ROLE_LOGIN This is a required role. An administrator with just ROLE_LOGIN is only allowed to view a few 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_USER_MANAGER An administrator with this role is allowed to “add users”, “delete users”, “edit users”, “select user certificates” and “select user signing certificate”.

ROLE_DOMAIN_MANAGER An administrator with this role is allowed to “add domains”, “delete domains”, “edit domains”, “select domain certificates” and “select domain signing certificate”.

ROLE_GLOBAL_MANAGER An administrator with this role is allowed to edit the global settings.

ROLE_LOG_MANAGER An administrator with this role is allowed to view the log files.

ROLE_PKI_MANAGER An administrator with 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 An administrator with this role is allowed to manage the queues (with the exception of the quarantine queue).

ROLE_SMS_MANAGER An administrator with this role is allowed to manage the SMS gateway.

ROLE_TEMPLATE_MANAGER An administrator with this role is allowed to edit templates.

ROLE_DLP_MANAGER An administrator with this role is allowed to manage all DLP settings like adding new DLP rules, removing DLP rules, managing the quarantine queue. In order to view the quarantine queue, the administrator also requires the **ROLE_QUEUE_MANAGER** role.

ROLE_QUARANTINE_MANAGER An administrator with this role is allowed to manage the quarantine queue. In order to view the quarantine queue, the administrator also requires the **ROLE_QUEUE_MANAGER** role.

21 Backup and restore

21.1 System backup

The backup manager can be used to backup and restore all the relevant system settings (including the certificates, keys and MTA settings). A backup can be created and downloaded to the administrators computer or a backup can be stored on a remote SAMBA share (see figure 74). A backup can be automatically initiated at set intervals and stored (encrypted or non encrypted) on a remote SAMBA share. A backup can be password encrypted. If no password is specified the backup will not be encrypted.

Warning: restoring a backup will overwrite all local settings and cannot be undone. The system will be restarted after the restore.

21.2 Backup configuration

The backup configuration page is used to configure the remote SAMBA share and configure the automatic backup (see figure 75).

System backup

backup config

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

Restore file
backup file to restore

Password
password for backup

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 74: System Backup

21.2.1 SMB share settings

The SMB share settings specify which remote SAMBA share should be used for remote backups (automatic backups can only be stored on a remote share). The remote share can be any server that supports the SMB protocol (for example Microsoft Windows Network or SAMBA). “Test connection” can be used to test whether the specified share can be accessed with the provided settings and credentials.

21.2.2 Automatic backup

Enabled Remote backups can be automatically initiated at set intervals. To enable automatic backups the “enabled” checkbox should be checked.

Cron expression The cron expression²⁴ determines at which intervals a backup will be started. The default cron expression `0 0 2 * * ?` automatically starts a backup every night at 2 o'clock (see Appendix D for more cron expression examples).

Password The password with which the backup will be encrypted.

21.2.3 Other

Strategy The filename of the backup is determined by the “strategy”. Choose between “day of week”, “day of month”, “day of year” and “timestamp”. “Day of week” uses the day of the week as a filename postfix (1-7). “Day of month” uses

²⁴For more info on the cron trigger format see <http://www.quartz-scheduler.org/docs/tutorials/crontrigger.html>

Backup configuration

SMB share settings

Domain
server domain

User Authenticate
user name

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

Password
backup password

General

Strategy
filename strategy

Cron expression examples

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

Figure 75: Backup configuration

Log export

log export config

The log export page allows you to export the log files. The logs can be exported to a remote SAMBA share or downloaded to the local computer. The exported file will be encrypted if the password is set.

Password encryption password
 last modified only export if modified in last minutes
 Export location Local Remote
The location of the exported logs

Figure 76: Log export

the day number as a filename postfix (1-31). “Day of year” uses the day (1-365) as a filename postfix. “Timestamp” uses a filename based on the number of milliseconds since January 1, 1970 UTC.

22 Log export

only available with the enterprise edition

With the log export, all system log files can be exported to a remote SAMBA share or downloaded to the local computer (see figure 76).

Password If a password is set, the exported logs will be PGP password encrypted.

Last modified If set, only log files which were modified within the last number of minutes will be exported. If not set, all logs files will be exported.

Export location The logs can be exported to the local computer (i.e., downloaded with the browser) or to a remote SAMBA share.

22.1 Log export config

The log export configuration page is used to configure the remote SAMBA share and configure automatic log export (see figure 77).

22.1.1 SMB share settings

The SMB share settings specify which remote SAMBA share should be used for remote log export (automatic log exports can only be stored on a remote

Log export settings

SMB share settings

Domain
server domain

User Authenticate
user name

Password
password for user

Server
server address

Port
server port

Share
name of the share

Directory
directory to use

Automatic log export

Enabled
auto export enabled

cron expression
export schedule

Password
encryption password

Automatic log export

Strategy
filename strategy

last modified
export if modified in
last n minutes

Cron expression examples

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

Figure 77: Log export settings

share). The remote share can be any server that supports the SMB protocol (for example Microsoft Windows Network or SAMBA). “Test connection” can be used to test whether the specified share can be accessed with the provided settings and credentials.

22.1.2 Automatic log export

Enabled Remote exports can be automatically initiated at set intervals. To enable automatic exports the “enabled” checkbox should be checked.

Cron expression The cron expression²⁵ determines at which intervals a log export will be started. The default cron expression `0 0 3 * * ?` automatically starts an export every night at 3 o’clock (see Appendix D for more cron expression examples).

Password The password with which the exported logs will be encrypted.

22.1.3 Other

Strategy The filename of the export is determined by the “strategy”. Choose between “day of week”, “day of month”, “day of year” and “timestamp”. “Day of week” uses the day of the week as a filename postfix (1-7). “Day of month” uses the day number as a filename postfix (1-31). “Day of year” uses the day (1-365) as a filename postfix. “Timestamp” uses a filename based on the number of milliseconds since January 1, 1970 UTC.

23 Reporting

only available with the enterprise edition

The gateway keeps statistics on all incoming and outgoing email like for example whether a message was encrypted. These statistics can be exported to a PDF report from the reporting page (Admin → reporting). The grouping (year, month, week, day), start date and end date can be specified (see figure 78).

Note: statistics are only persisted to the database if the number of cached entries exceeds a fixed limit. This is done to minimize the number of database writes required when handling an email. It will therefore take a number of emails before the reporting functionality returns updated statistics.

23.1 Report

A PDF report shows the statistics grouped by date (see figure 79). The statistic for email sent to internal recipients (recipients with locality set to “Internal”)

²⁵For more info on the cron trigger format see <http://www.quartz-scheduler.org/docs/tutorials/crontrigger.html>

Reporting

The generated PDF will contain information about the number of sent and received e

Report

Group by

From date

To date

Figure 78: Reporting

starts with “incoming” and the statistic for email sent to external recipients starts with “outgoing”.

24 SSL/TLS

24.1 Web GUI

Access to the Web GUI and portal is protected with SSL/TLS. During installation, a default SSL certificate has been installed²⁶. It is therefore advised to install a new SSL certificate after installation. On the “SSL/TLS configuration for the web GUI” page, a new SSL certificate can be imported (see figure 80). A password protected “PKCS#12” file (.pfx or .p12) with the SSL certificate and private key suitable for SSL should be uploaded. After installation of the SSL certificate, the system must be restarted. The system can be restarted by clicking “Restart” on the “SSL certificate manager” page or by opening the “Admin” menu and selecting “Restart” on the left hand side menu²⁷.

Note: if the PDF portal functionality (like for example the PDF reply) is used you are advised to install an SSL certificate which is trusted by all browsers (for example Comodo, Verisign or StartSSL certificates).

24.2 SMTP

only available with the enterprise edition

²⁶With the virtual appliance, a new SSL/TLS certificate is generated when the appliance is started for the first time

²⁷Alternatively with the Virtual Appliance, the system can be restarted by selecting “Restart services” from the Virtual Appliance Console.

CipherMail report	
Grouped by month	
Date	2015-05-01
incoming-external	1223
incoming-external-recipients	1230
incoming-internal	3368
incoming-internal-recipients	3368
incoming-pgp-encrypted	7
incoming-pgp-encrypted-recipients	7
incoming-smime-encrypted	21
incoming-smime-encrypted-recipients	21
outgoing	4657
outgoing-pgp-encrypted	44
outgoing-pgp-encrypted-recipients	44
outgoing-recipients	4664
outgoing-smime-encrypted	1084
outgoing-smime-encrypted-recipients	1084
outgoing-webmail-encrypted	4
outgoing-webmail-encrypted-recipients	4
Date	2015-06-01
incoming-external	1806

Figure 79: Report

SSL/TLS configuration for the web GUI

The Web GUI is protected with SSL/TLS. On this page a new SSL server certificate for the file.

Note: after uploading a new SSL certificate, the server has to be restarted.

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

Password
password of the private key file

Figure 80: SSL/TLS configuration for the web GUI

TLS configuration for the SMTP server

The SMTP server can protect the transport layer with TLS (formerly known as SSL). The server certificate and private key are uploaded as a password protected PFX file. If the server certificate and key are

Private key file No file selected.
the file (.pfx/.p12) containing the
TLS certificate and private key.

Password
password of the private key file

Figure 81: TLS configuration for the SMTP server

The SMTP server supports TLS for incoming and outgoing SMTP. During installation a new SSL/TLS certificate is generated when the appliance is started for the first time. On the “TLS configuration for the SMTP server” page, a new SSL certificate can be imported (see figure 81). A password protected “PKCS#12” file (.pfx or .p12) with the SSL certificate and private key suitable for SSL should be uploaded. The SMTP server will be automatically restarted after the installation of the new SSL certificate.

24.3 CSRs

only available with the enterprise edition

For the portal functionality, it's advised to use a certificate which is trusted by all browsers. This requires that the certificate is issued by a trusted CA (for example Comodo, Verisign or StartSSL). The certificate with private key can be imported using a password protected “PKCS#12” file. This however requires that a “PKCS#12” file is already available. The “Certificate Signing Requests” page can be used to request a certificate from an external trusted CA (see figure 82).

24.3.1 CSR manager

Most CAs require a Certificate Signing Request (CSR) before they can issue a certificate. When a CSR is generated, a private/public key pair is generated together with some identifying information (for example the name of the company). After generating the CSR, the CSR should be sent to the CA. The CA will then create a new certificate using the data from the CSR. This certificate should then be imported into the CSR store. The certificate will then be combined with the associated private key and the certificate and private key can be exported to a password protected PKCS#12 file. The CSR store stores the generated CSRs together with the associated private keys. CSRs for which the certificate is not yet imported are shown in yellow (see figure 82). CSRs for

Certificate Signing Requests

A certificate signing request (CSR) is used by a certificate authority (CA) to issue a trusted SSL/TLS certificate. The generated CSR should be sent to the CA. The CA will then create a new certificate using the data from the CSR. The certificate should be imported into the CSR store. Once a certificate is imported, the certificate and private key can be exported to a password protected PKCS#12 file.

[create new CSR](#) | [download CSRs](#) | [download certificates](#) | [delete selected](#)

	ID	Date	Subject	Key Length
✘	<input type="checkbox"/> 0f122bfd-55e9-405c-8632-f9b2b68f8d66	08/19/2015 11:34	E=test@example.com,CN=Test CSR	2048
✘	<input type="checkbox"/> 7e728e5e-337f-42f3-a524-5242708ebde9	08/19/2015 11:35	E=test@example.com,CN=Test CSR 2	2048

Certificate not imported ■

Certificate file No file selected.

Figure 82: Certificate Signing Requests

which the certificate was imported, can be exported to a password protected PKCS#12 file by selecting the CSRs and clicking “download certificates”.

24.3.2 Certificate request procedure

The following steps will outline the procedure with which a trusted SSL certificate can be requested for the Web GUI:

1. Create a CSR
2. Download CSR
3. Send CSR to CA
4. Import certificate generated by CA
5. Download certificate as password protected “PKCS#12” file
6. Import “PKCS#12” file into Web GUI

1. Create A CSR Click “Create new CSR” on the “Certificate Signing Request” page (see figure 82). On the “Create certificate signing request” page (see figure 83), fill in the request details required by the CA and select the length of the private key. A public/private key pair will be generated and the CSR will be created when the “Create” key is pressed. The CSR together with the public/private key pair will be stored in the CSR store.

2. Download CSR Select the CSR, and click “Download CSRs”. Save the downloaded CSR.

3. Send CSR to CA Send the downloaded CSR to the CA. It depends on the CA how the CSR should be delivered to the CA.

Create a new certificate signing request

Certificate subject

Email

Common name
required

more

Organization

First name

Last name

Key length
in bits

Figure 83: Create certificate signing request

4. Import certificate generated by CA The CA will generate a certificate using the details from the CSR ²⁸. After the CA has issued the certificate, import the certificate into the CSR store. After import the certificate, the certificate and private key belonging to the certificate will be combined.

5. Download certificate as password protected “PKCS#12” file Select the CSR for which the certificate and private should be exported to a “PKCS#12” file and click “download certificate”. On the “Export CSR certificates and keys” page, a password for the “PKCS#12” file should be provided.

6. Import “PKCS#12” file into Web GUI The exported password protected “PKCS#12” file can now be imported into the Web GUI. See section 24 for details on how to import the “PKCS#12” file.

25 Remote monitoring

only available with the enterprise edition

The gateway can be remotely monitored using the monitoring web service. The monitoring web service is accessible on https://HOST/unprotected/monitor/*?password=PASSWORD where * should be replaced with the name of the service to monitor. For example the following URL returns the number of mails in the MTA queue:

<https://HOST/unprotected/monitor/mta-queue-size?password=PASSWORD>

²⁸Generating a certificate may take a few seconds or a couple of days. This depends on the policies of the CA.

Monitoring settings

Allow access to the remote monitoring service only from a specific IP range

Remote monitoring

Enabled
remote monitoring enabled

IP filter
space or comma separated list of IP ranges

Password
password for the remote monitor service

Figure 84: Monitoring configuration

Note: HOST and PASSWORD should be replaced with the real hostname and configured password for the monitoring service.

For more details on the supported commands and their return values, see the separate monitoring guide.

25.1 Monitoring configuration

The monitoring configuration (Admin → other → monitoring) can be configured on the “Monitoring configuration” page (see figure 84). The monitoring service should be enabled, the IP address from which the connection is made should be allowed and the password for the monitoring service should be set. If the monitoring service is not enabled or if the IP address is not authorized or the password is not set or not correct, an “access denied” page is shown. The authorized IP addresses (IP filter) can be set to multiple comma separated IP addresses or to some IP range in CIDR format. For example: 192.168.88.0/24, 10.0.0.16

26 Certificate request by mail

only available with the enterprise edition

A problem with S/MIME is that in order to encrypt email, the certificate of the recipient must be available. One option to get someone’s certificate is by

asking the recipient to send a digitally signed email. The gateway will extract the certificate from the digitally signed message and import it into the gateway. With the “Certificate request by mail” option, the gateway can be configured to automatically reply with a digitally signed email to an incoming email. This can be used by external senders to “automatically” retrieve a certificate from the gateway which can then be used for sending S/MIME encrypted email. Because the reply is digitally signed, the email client (for example Outlook) can extract the certificate from the digitally signed email.

The automatic reply service will only be active if it is enabled and if the sender used a subject for the mail which matches a pre-defined regular expression and if the message was digitally signed with a trusted certificate (this can be disabled). The “Certificate request by mail” service can be configured on the Certificate request by mail page (see figure 85). The configuration can be changed for the global settings, domain or for an individual recipient.

Enabled The “Certificate request by mail” service is only enabled if “Enabled” is checked.

Subject trigger The “Subject trigger” is a regular expression which will be matched against the subject of an incoming email. If matched, the message will be handled by the “Certificate request by mail” service.

Must be signed If checked (the default), the message will only be accepted if the incoming message was signed with a trusted digital S/MIME signature.

26.1 Certificate request by mail reply templates

The digitally signed reply messages are based on the “Cert request signed” and “Cert request not signed” templates. The templates can be modified by the administrator (see section 7). The reply template “Cert request signed” is used if the email is accepted and there is a valid signing certificate. The reply template “Cert request not signed” is used if the email is accepted but there is not a valid signing certificate.

Note: if the email contains the subject trigger and is signed, or not signed if “Must be signed” is not enabled, the email will “not” be delivered to the recipient. The email will be handled by the gateway and the reply (based on the template “Cert request signed” or “Cert request not signed”) will be sent. It’s therefore important that the subject pattern used is not something that is triggered by normal emails.

27 Proxy

For downloading of CRLs and sending of SMS Text messages, the gateway needs access to external resources. If external resources should be accessed via a proxy, the proxy client should be configured. The proxy client only supports HTTP(s) and “NTLMv1” (“NTLMv2” is not supported). The proxy client

Certificate request by mail settings for global preferences

Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/> inherit
Subject trigger (regular exp.)	<input type="text"/>	<input checked="" type="checkbox"/> inherit
Must be signed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> inherit

Apply Close

Figure 85: Certificate request by mail

Proxy configuration

The proxy settings will be used for all HTTP(S) access (downloading CRLs over HTTP(s),

Username
proxy username

Password
proxy password

Domain
for NTLMv1

Host
proxy Host

Port
proxy Port

Enabled

Apply Cancel

Figure 86: Proxy configuration

can be configured by opening the “Admin” page and selecting “Proxy config” (see figure 86).

28 Fetchmail

Fetchmail can be used to retrieve email from remote “POP3”, “IMAP” servers. The retrieved email can then be forwarded to some other email addresses by the Ciphermail gateway. The servers from which email should be fetched and the email addresses to which email should be forwarded to can be configured with the fetchmail configuration page.

Note: Fetchmail support is only available on the Virtual Appliance²⁹.

²⁹Contact us for instructions on how to enable Fetchmail support for a non-appliance version of the Ciphermail gateway.

28.1 Fetchmail manager

When Fetchmail support is enabled a “Fetchmail manager” option is added to the admins menu (see figure 87). With the “Fetchmail manager” page new servers can be added which will be periodically polled for new messages (see figure 88).



The screenshot shows a web interface titled "Admins". Below the title is a navigation bar with links: "Backup manager | MTA config | Fetchmail manager | JCE pol". Below the navigation bar is a table with three columns: "Username", "Enabled", and "Roles". The table contains one row with the following data:

Username	Enabled	Roles
admin	true	ROLE_LOGIN, ROL

Figure 87: Admins fetchmail options

28.1.1 Global settings

Fetchmail manager contains three global settings relevant for all polled servers: “Postmaster”, “Poll interval” and “Check certificate”.

Postmaster If email cannot be forwarded an error message will be sent to the postmaster email address.

Poll interval The number of seconds between consecutive checks for new email. For “IMAP” accounts with “IDLE” support a new message is instantly detected and forwarded (also known as push mail). The “Poll interval” should not be too low to prevent flooding of the remote server.

Check certificate If checked, Fetchmail checks whether the server certificate is trusted and is issued by a locally trusted CA.

28.1.2 Applying changes

When the “Apply” button is pressed the Fetchmail configuration will be updated and Fetchmail will be restarted.

28.1.3 Adding a new account

New accounts to be polled and forwarded can be added by clicking “add account” (see figure 88). The page “Fetchmail Add Account to Poll” will be opened (see figure 89). The account settings will be briefly explained.

Server The server that is being polled. This can be a fully qualified domain name or an IP address.

Fetchmail Manager

[add account*](#) | [delete selected*](#) | [invert selection](#)

There are no entries

Postmaster
email address of the last-resort recipient

Poll interval
background poll interval in seconds

Check certificate
only accept trusted server certificates

* after adding or deleting fetchmail accounts, the settings should be applied

Apply Close

Figure 88: Fetchmail manager

Port The port the server being polled listens on. If left empty the default port for the protocol will be used.

Protocol The protocol of the server being polled (“POP3”, “IMAP” etc.).

Authentication The authentication protocol the server being polled uses. With “Any”, Fetchmail tries each available method consecutively until a successful login.

Principal The Kerberos principal (only relevant for IMAP and kerberos).

Username The username of the remote account.

Password The password of to the user account.

Folder The remote folder to query.

UIDL Force client-side tracking of new messages. Should be used in conjunction with “keep”. This setting is only relevant for “POP3”.

SSL Connect to the remote server via SSL.

Keep If “Keep” is selected, seen messages are not deleted from the remote server (if “Keep” is used with “POP3”, “UIDL” should also be selected). If possible, seen message should be deleted to make sure a message is never delivered twice. It is therefore advised to leave “Keep” unchecked.

Idle If selected, Fetchmail waits for new messages after each poll (IMAP only). With “Idle” new messages are instantly forwarded.

Forward To The email address to forward newly polled messages to.

29 System runtime control

The “System runtime control” page can be used to manage the runtime of the gateway (rebooting, and start/stopping the MTA etc. see figure 90). The “System runtime control” page can be opened by clicking Admin → system.

30 Compose test email

The “Compose test email” page can be used to create a test email to test the gateway settings (see figure 91). The “Compose test email” page can be opened by clicking Admin → other → send email.

31 Extract text from a MIME message

With the “Extract text from a MIME message” page, the text from an uploaded email will be extracted and returned (see figure 92). This allows the administrator to see which text the DLP scanner uses for pattern matching. This helps the administrator to create DLP rules. The “Extract text from a MIME message” page can be opened by clicking Admin → other → extract text.

Fetchmail Add Account to Poll

Server
server address

Port
server port

Protocol
server Protocol

Authentication
authentication type

Principal
Kerberos principal
(IMAP and kerberos only)

Username
user account

Password
password for the user

Folder
remote folder to query

UIDL
force POP3 to use client-side UIDLs

SSL
connect to server using SSL encryption

Keep
leave messages on server

Idle
idle waiting for new messages after each poll (IMAP only)

Forward To
email address to forward to

Figure 89: Fetchmail new account

System runtime control

Gateway

Restart the gateway by pressing the restart button. Restarting will take approximately 45 seconds.

Restart

Reboot the gateway by pressing the reboot button. Rebooting will take approximately 120 seconds.

Reboot

Shutdown the gateway by pressing the shutdown button.

Shutdown

MTA

Status: **running** ✓

Stop the Mail Transfer Agent.

Stop MTA

Start the Mail Transfer Agent.

Start MTA

Close

Figure 90: System runtime control

Compose a test email

On this page, a test email can be composed which will be handled by the gateway. Multiple recipients should be UTF-8 encoded.

To
recipients

Cc
cc recipients

Bcc
bcc recipients

From
from (header)

Sender
envelope sender

Subject
email subject

Additional Headers
name:value pairs

Body (max 4096 characters)

Figure 91: Compose test email

Extract text from a MIME message

A MIME encoded email can be uploaded from which the DLP engine will extract text from an email before scanning.

MIME message
email (max. 10 MB)

Figure 92: Extract text

A SMTP HELO/EHLO name

The SMTP helo/ehlo name is the hostname the SMTP server sends with the SMTP EHLO or HELO command (the Ciphermail gateway uses the HELO or EHLO command when sending email to another email server). Some email servers check whether the helo/ehlo name is equal to the reverse IP lookup (with a reverse IP lookup the name is retrieved that belongs to the IP address) and if the names do not match they will flag the email as spam.

If the Ciphermail gateway is used to directly send email to external recipients (i.e., outgoing email is not relayed through an external relay host) the gateway should be setup with the correct helo/ehlo. The SMTP helo name should be equal to the reverse lookup of the external IP address.

If the external IP address is not known and the Ciphermail gateway uses the same IP address as the web browser, the external IP address and hostname (reverse IP) can be retrieved using on-line services like <http://www.whatismyipaddress.com>. The IP address shown is the external IP address. The shown hostname (the reverse IP lookup) should be used for the SMTP helo name. If the hostname of the Ciphermail gateway is set to the external hostname, the SMTP helo name can be left empty because the SMTP helo name will then be equal to the gateway hostname.

Checking the HELO/EHLO name whether the HELO/EHLO name is correctly setup can be checked using the helo check services from <http://cbl.abuseat.org/helocheck.html> by sending an email to “helocheck@cbl.abuseat.org”. The email will be immediately bounced. The bounce message contains the HELO name used by the gateway.

```
<helocheck@cbl.abuseat.org>: host mail-in.cbl.abuseat.org said:
    550 HELO for IP 82.94.189.170 was "secure.djigzo.com"
    (in reply to RCPT TO command)
```

Where 82.94.189.170 is the external IP address of the gateway (IP address will be different for every server) and “secure.djigzo.com” was the HELO name used by the gateway.

B SASL authentication

SMTP client authentication is not enabled by default. SMTP client authentication can be enabled by adding the following lines to the postfix main config using the “MTA raw config” page (see 4.4).³⁰

```
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/smtp_client_passwd
smtp_sasl_type = cyrus
```

New SASL credentials for an SMTP host can be added by clicking “add password”. This opens the “Add SASL password” page (see figure 93). If “mx”

³⁰The main config that comes with Ciphermail gateway already contain these lines. They are however commented out.

is selected the MX-records of the server are used instead of the IP address of the server (A-record). In most cases the IP address of the server should be used and “mx” should therefore not be selected.

Figure 93: SASL add password

Gmail example: as an example the following part will explain how to use the Gmail SMTP servers as an external relay host (i.e., email sent to external recipients will be relayed via Gmail). For SMTP authentication Gmail requires a TLS protected connection. TLS and sasl authentication should therefore be enabled by adding the following lines to the postfix main config file using the “MTA raw config” page (see 4.4):

```
smtp_tls_security_level = may
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/smtp_client_passwd
smtp_sasl_type = cyrus
smtp_tls_CApath = /etc/postfix/certs/
smtp_sasl_security_options =
```

The “External relay host” should be set to “smtp.gmail.com” and the port to “587” (see figure 94).

Figure 94: Gmail external relay host

The SASL password for server “smtp.gmail.com” and port “587” should be set. The username should be set to the Gmail username (the username should include @gmail.com) and password (see figure 95).

SASL passwords*

add password | delete selected | invert selection

	Server	Port	Mx Lookup	Username	Password
<input type="checkbox"/>	smtp.gmail.com	587	false	test	***

* smtp client authentication is only active when sasl is enabled.

Apply Close

Figure 95: Gmail SASL password

C Content and virus scanning

A content scanner can be used in combination with Ciphermail gateway to selectively force encryption when a message contains certain keywords (for example a “Social Security Number”). A typical setup of a content scanner and an encryption gateway can be see in figure 96.

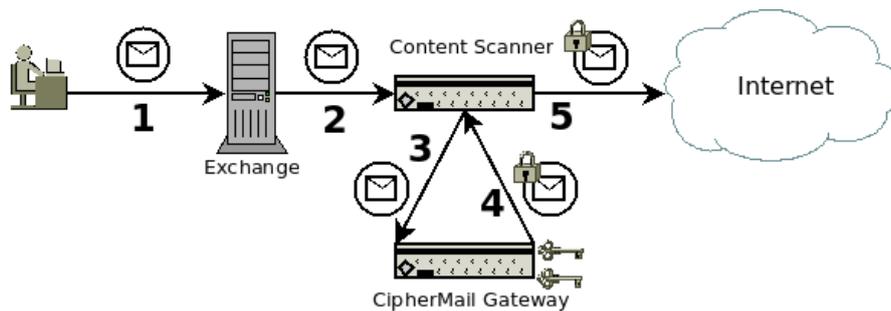


Figure 96: Content scanning

Ciphermail gateway with content scanner:

1. User sends unencrypted message.
2. Exchange forwards message to content scanner.
3. Content scanner detects that the message must be encrypted (for example the message contains a SSN).
4. Ciphermail gateway encrypts the message with S/MIME or PDF.
5. Content scanner sends the encrypted message to the recipient.

Most organizations need to scan all incoming and outgoing email for viruses. A typical setup of an encryption gateway and a virus scanner can be see in figure 97.

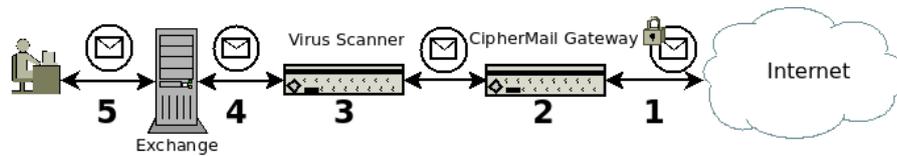


Figure 97: Virus scanning

Ciphermail gateway with virus scanning:

1. S/MIME encrypted message is received from the Internet.
2. Ciphermail gateway decrypts the message.
3. The decrypted message is scanned for viruses.
4. After virus scanning the message is forwarded to Exchange.
5. User reads the message.

A more advanced setup is required when email must be encrypted on the desktop yet all outgoing email must be virus scanned because of corporate policies. Figure 97 shows how encrypted outgoing email can be virus scanned.

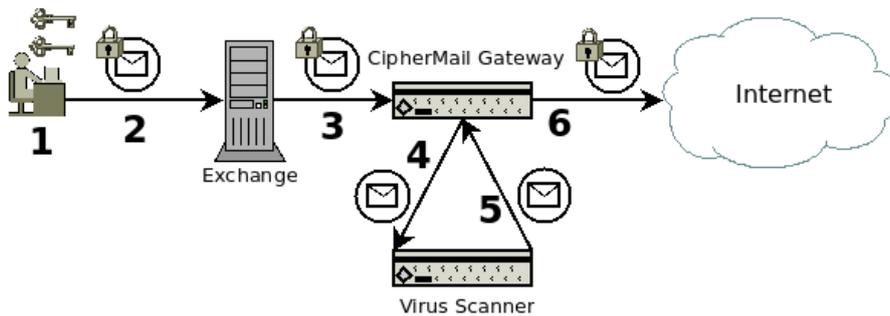


Figure 98: Virus scanning with desktop encryption

Ciphermail gateway with desktop encryption and virus scanning:

1. User encrypts message with personal and receivers certificate.
2. S/MIME encrypted message is sent to Exchange.
3. Exchange sends S/MIME encrypted message to the Ciphermail gateway.
4. Ciphermail gateway decrypts the message with the senders private key (the gateway stores a copy of the key) and sends the decrypted message to the virus scanner.
5. Virus scanner scans the message and if clean it will be sent back to the Ciphermail gateway.
6. The Ciphermail gateway re-encrypts the message and sends the message to the external recipient.

D Cron Expressions

The following cron examples are taken from <http://www.quartz-scheduler.org/docs/tutorials/crontrigger.html>.

Expression	Meaning
0 0 12 * * ?	Fire at 12pm (noon) every day
0 15 10 ? * *	Fire at 10:15am every day
0 10,44 14 ? 3 WED	Fire at 2:10pm and at 2:44pm every Wednesday in March.
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

For more cron examples see the “Quartz Scheduler” website.

E MPA mail flow

The following flow-charts will show exactly how email is processed by the Ciphermail gateway.

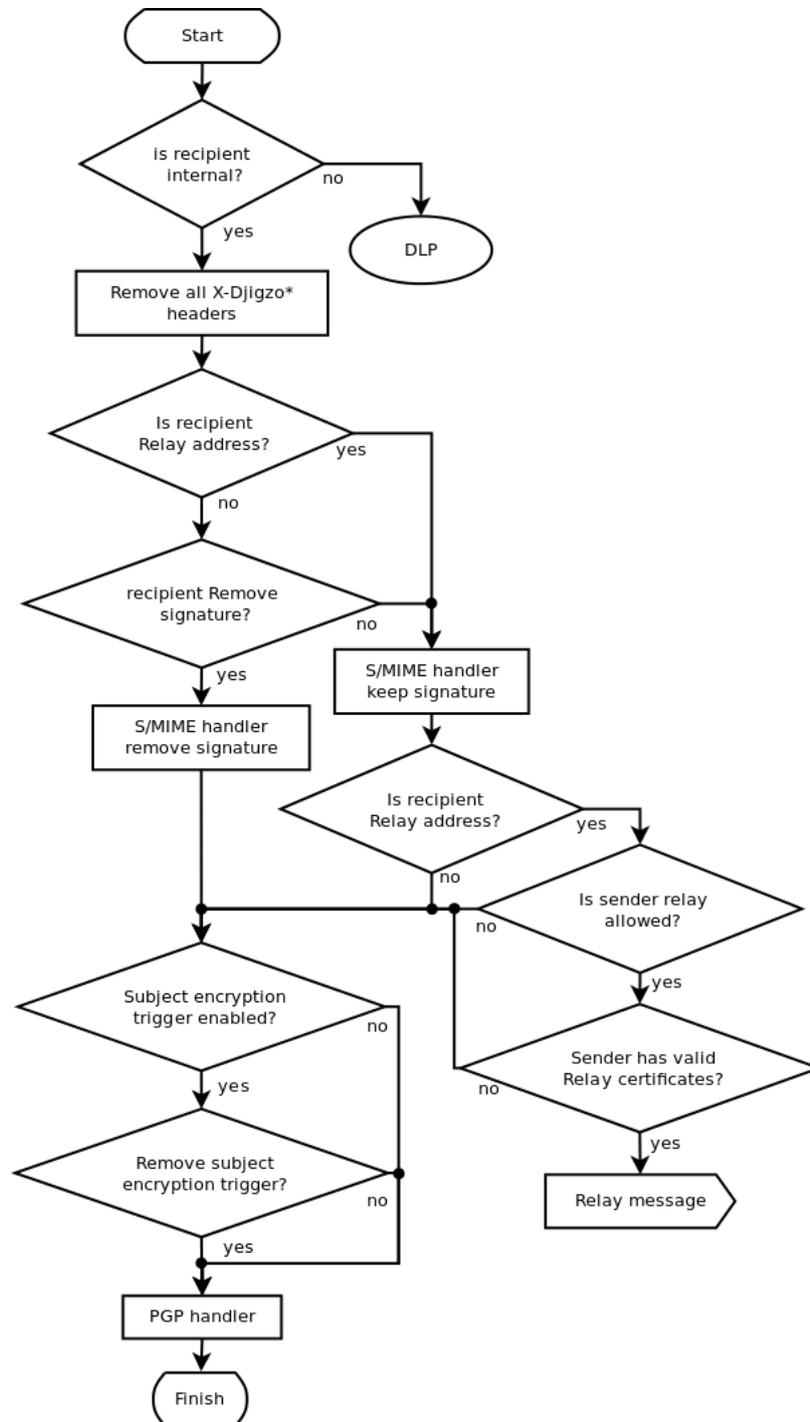


Figure 99: Start

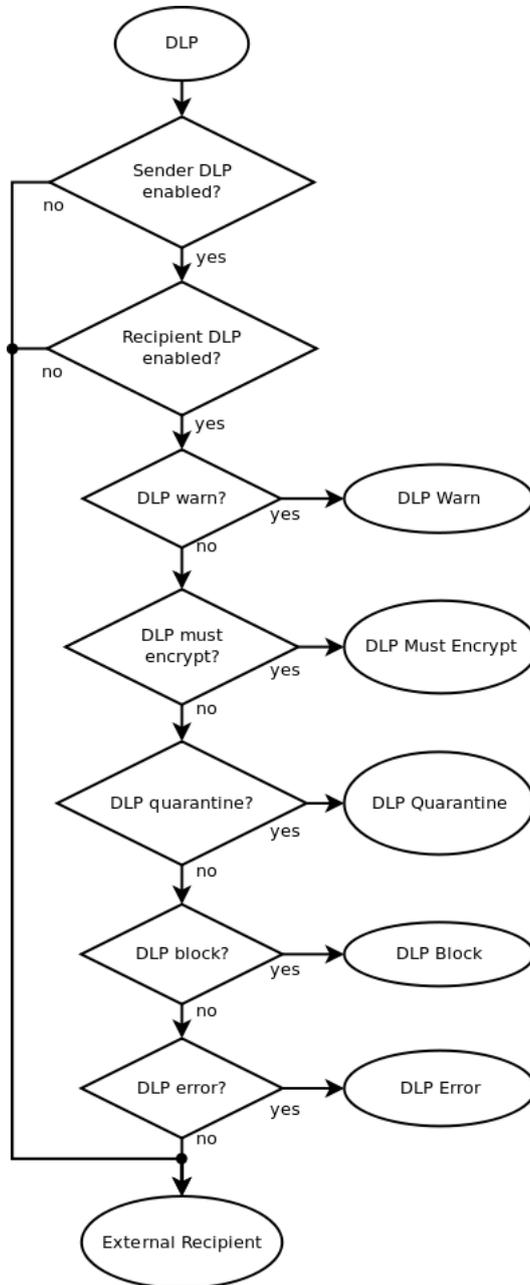


Figure 100: DLP

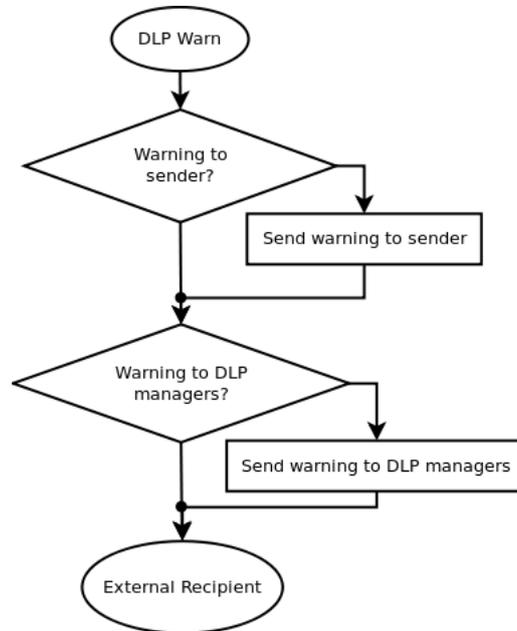


Figure 101: DLP Warn

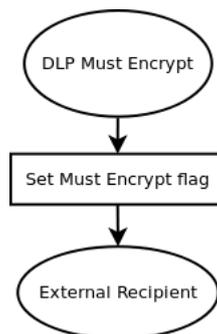


Figure 102: DLP Must Encrypt

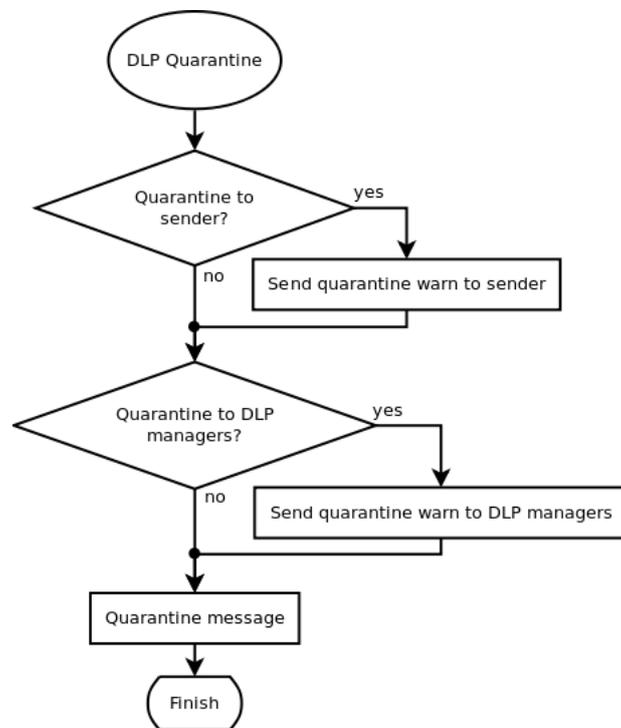


Figure 103: DLP Quarantine

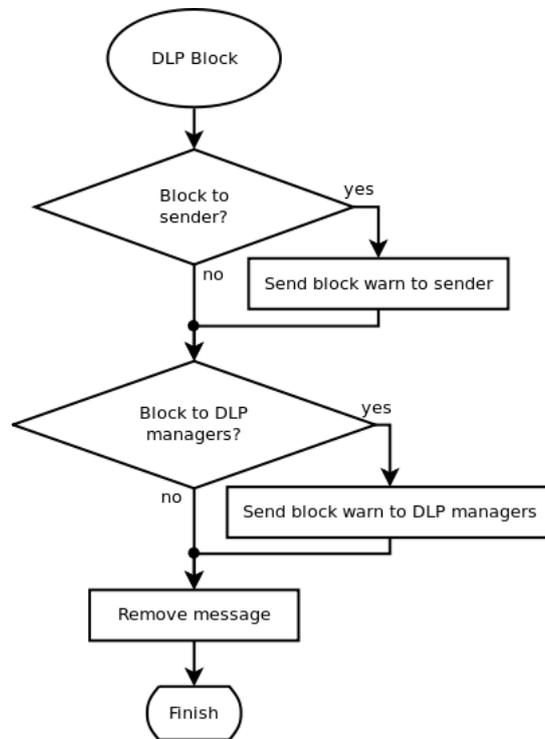


Figure 104: DLP Block

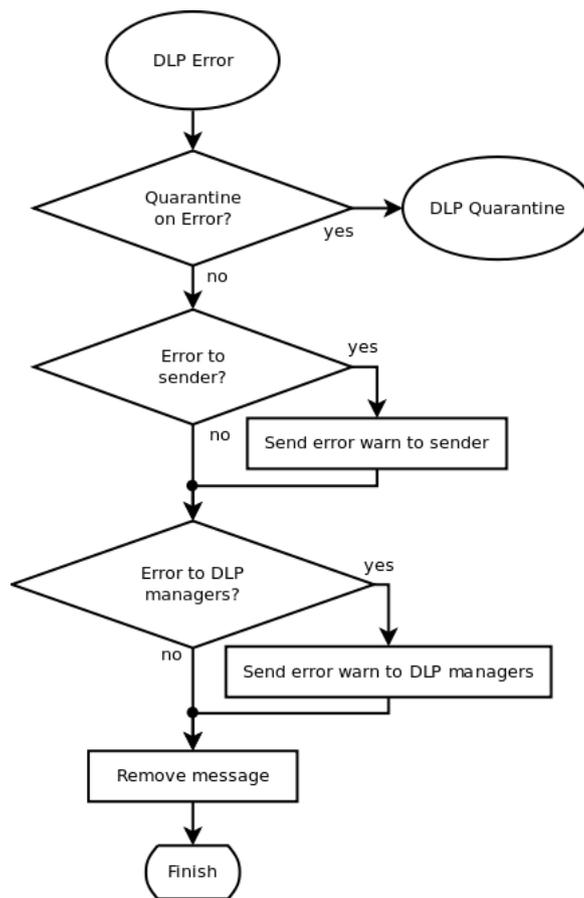


Figure 105: DLP Error

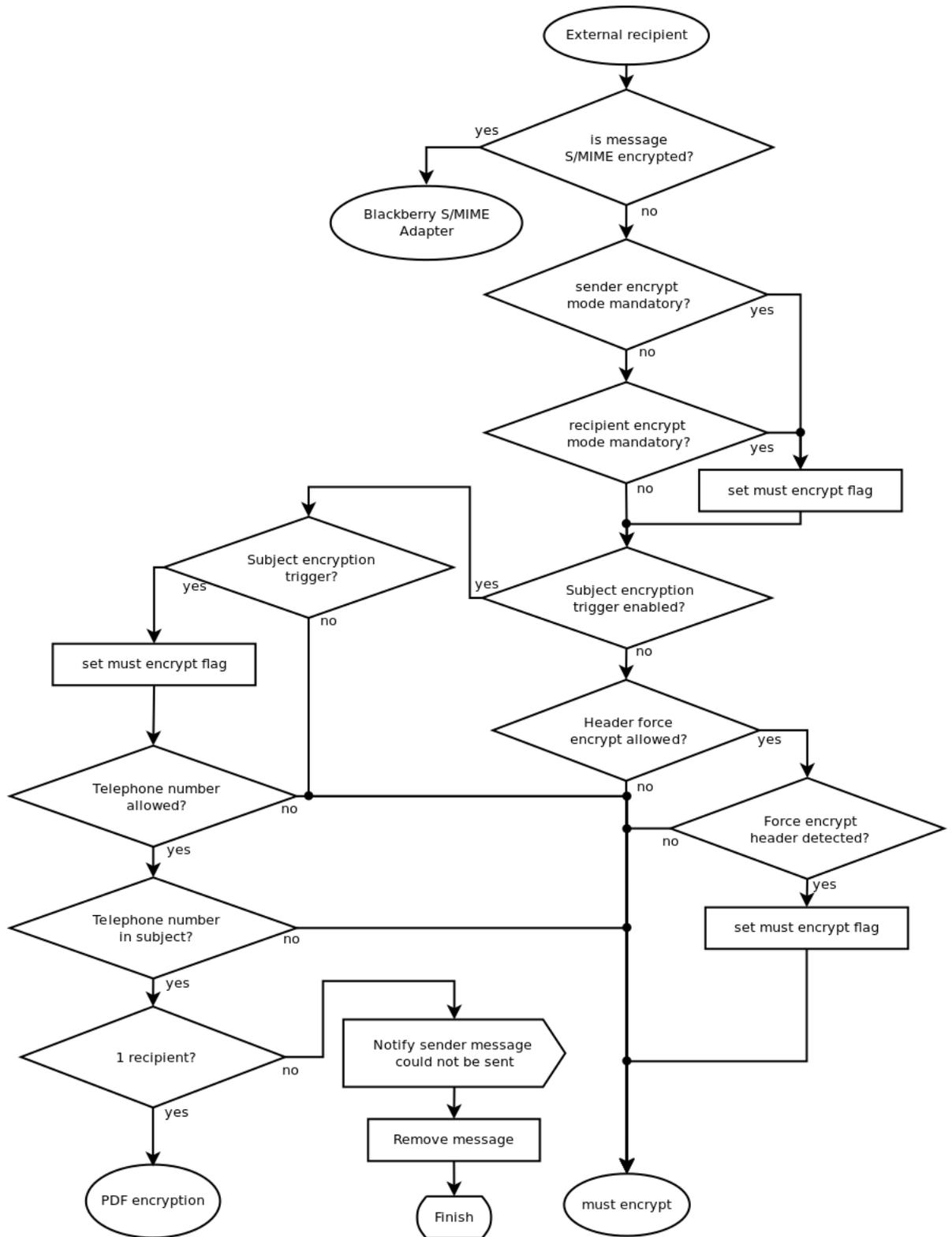


Figure 106: External recipient

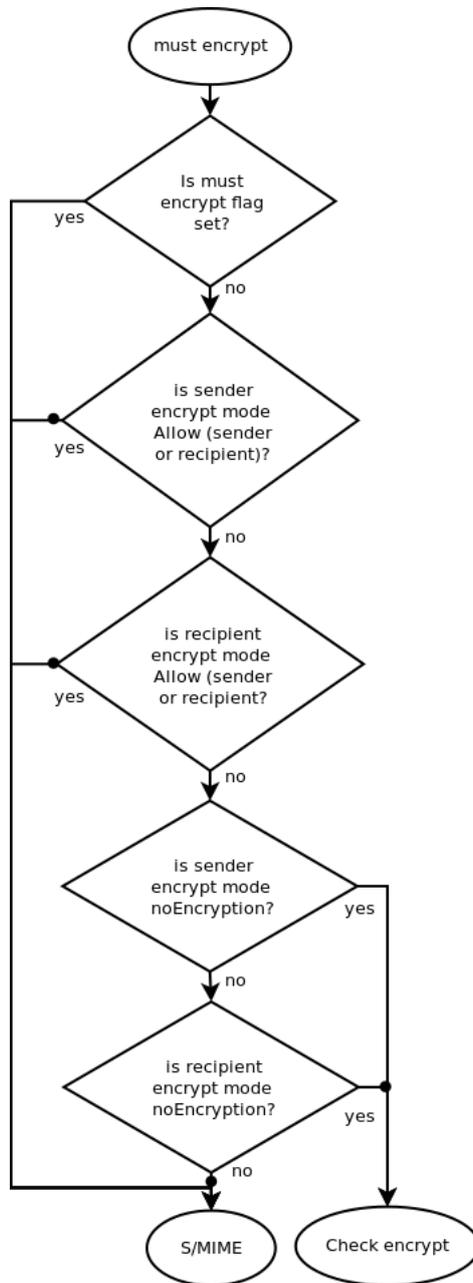


Figure 107: Must encrypt

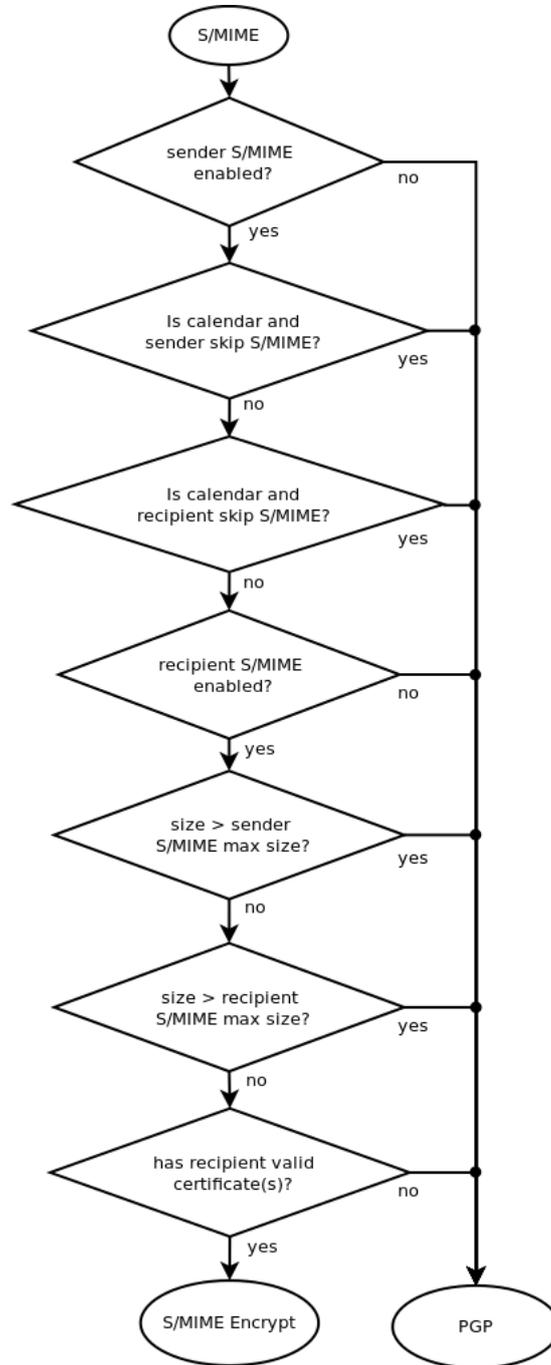


Figure 108: S/MIME

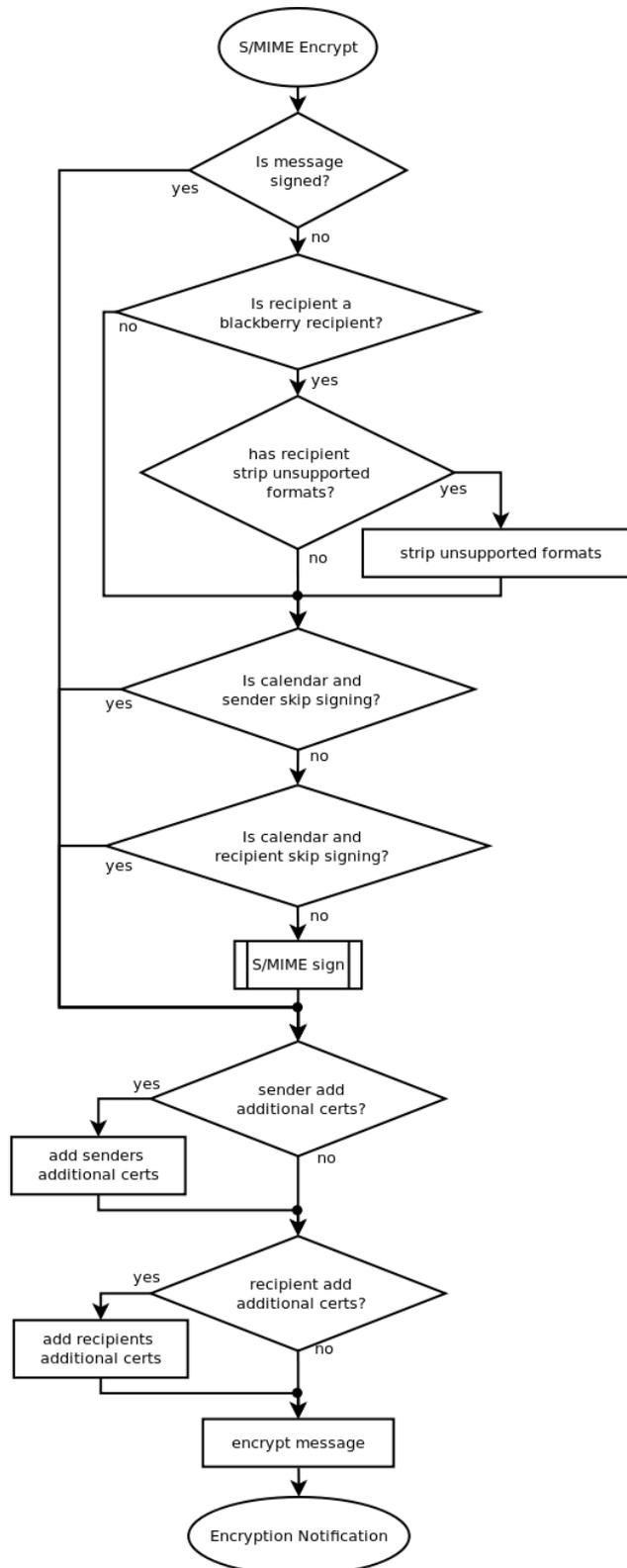


Figure 109: S/MIME encrypt
128

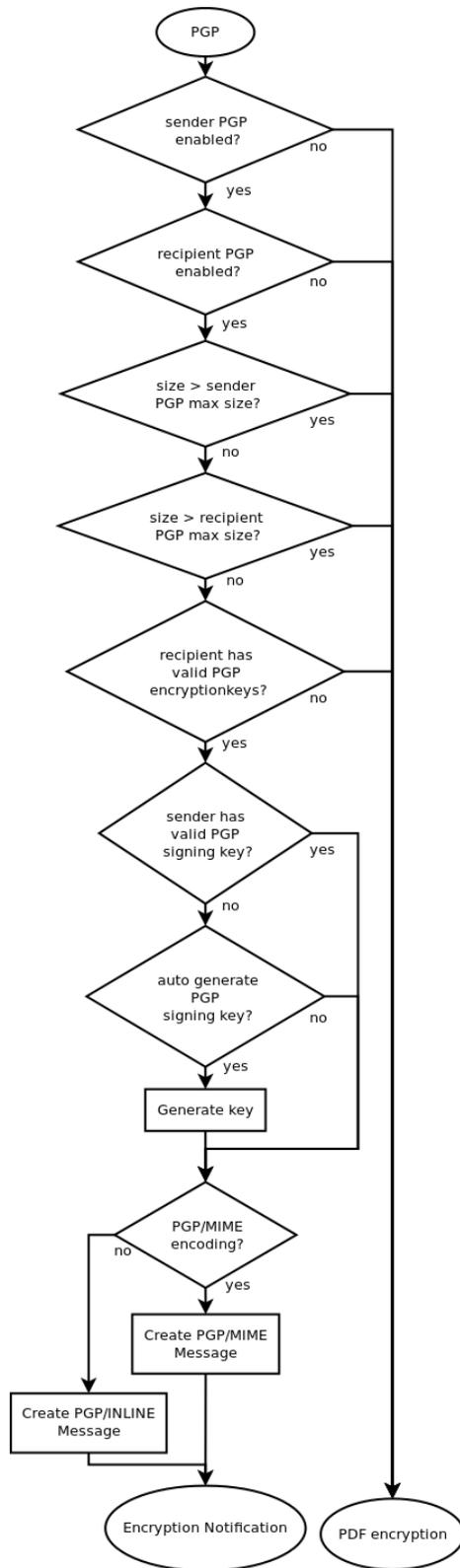


Figure 110: PGP
129

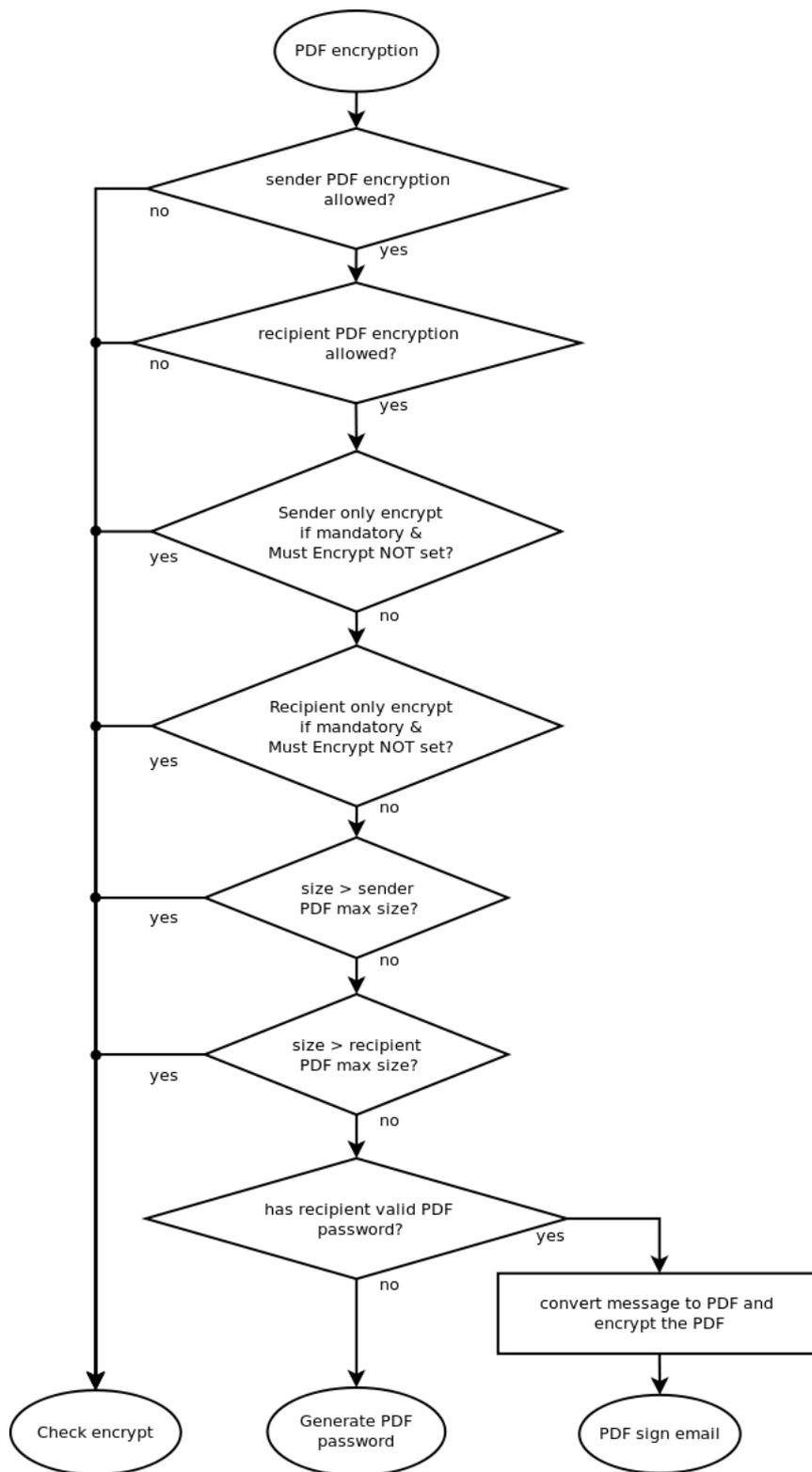


Figure 111: PDF encryption

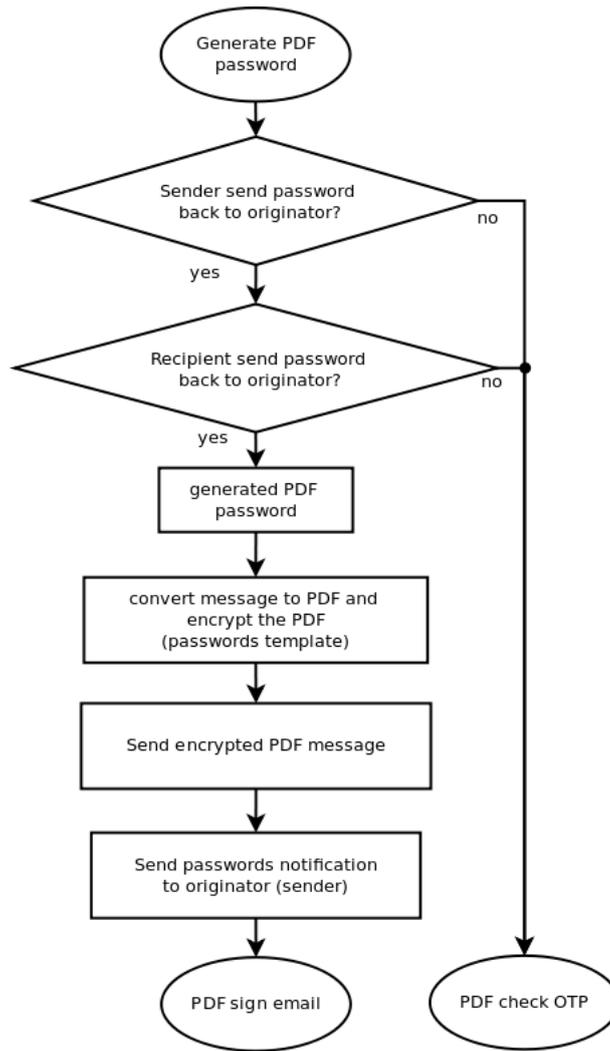


Figure 112: Generate PDF password

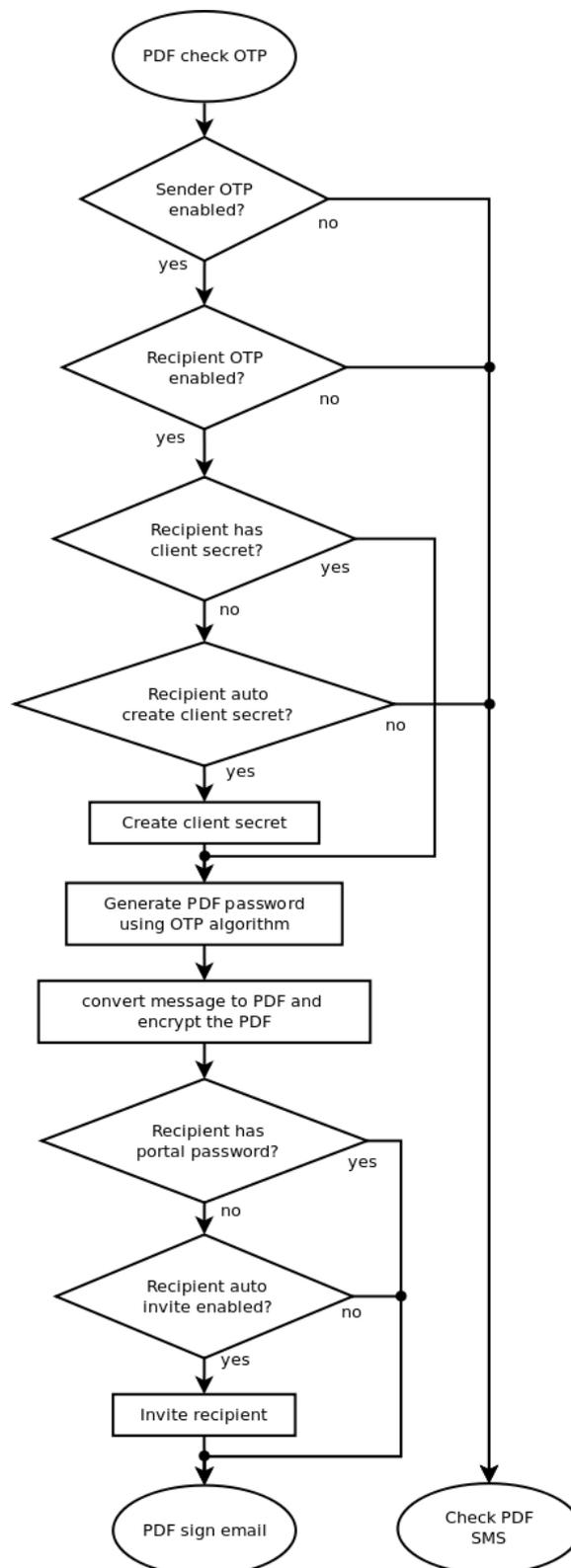


Figure 113: Check PDF OTP
132

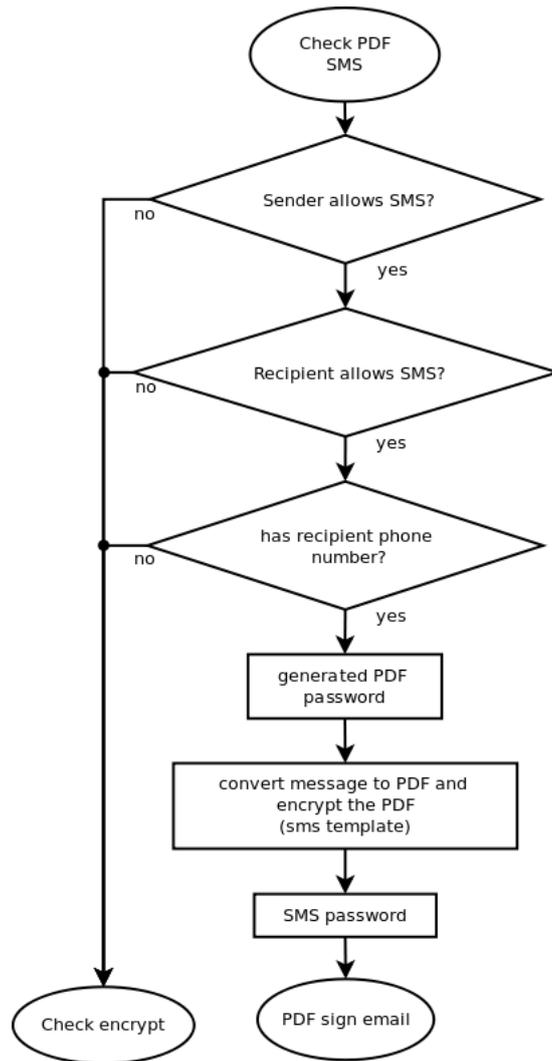


Figure 114: Check PDF SMS

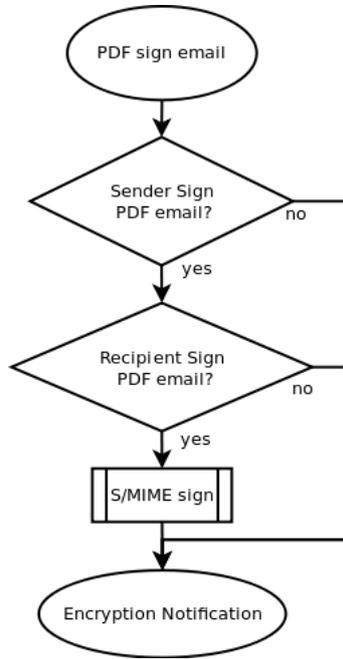


Figure 115: PDF sign email

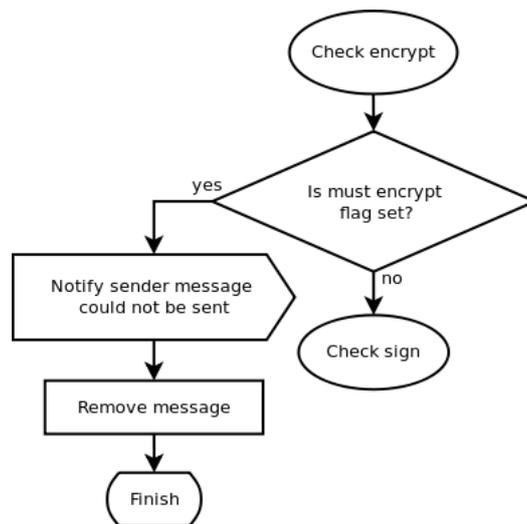


Figure 116: Check encrypt

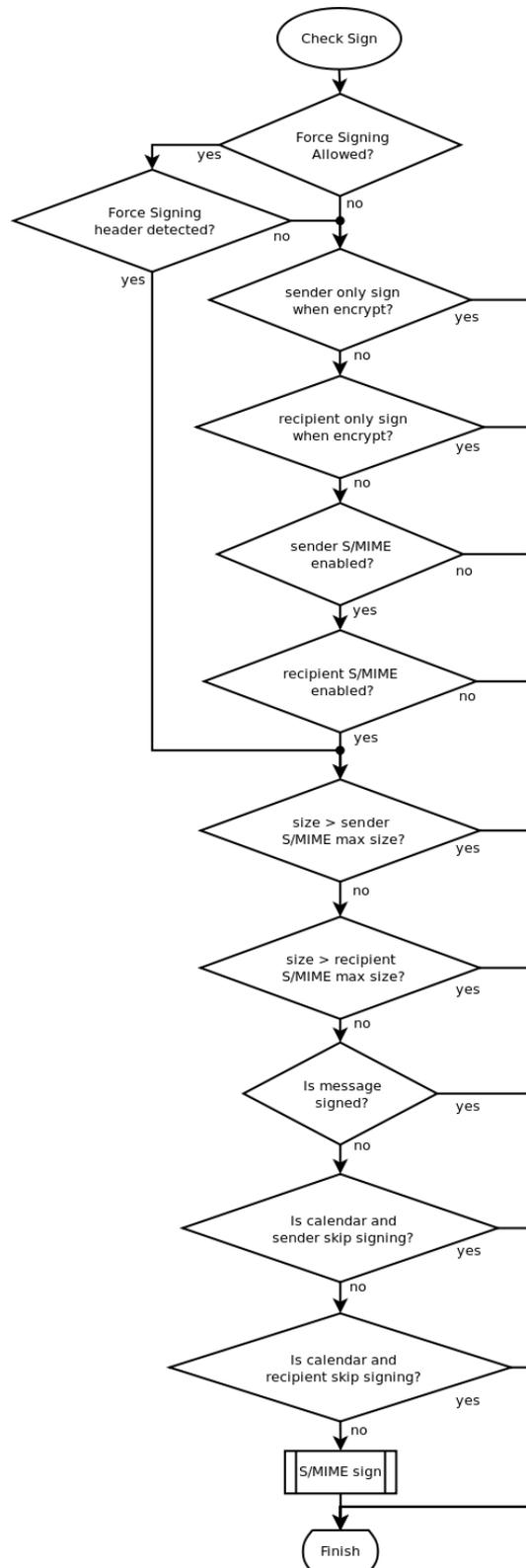


Figure 117: Check Sign
135

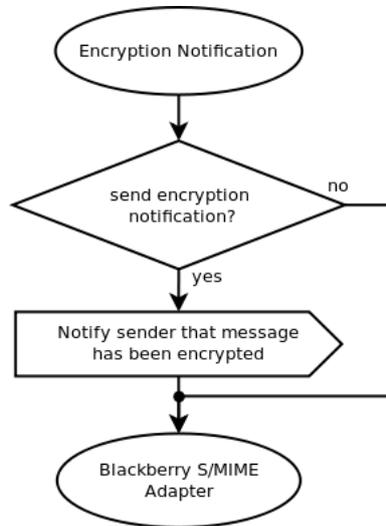


Figure 118: Encryption notification

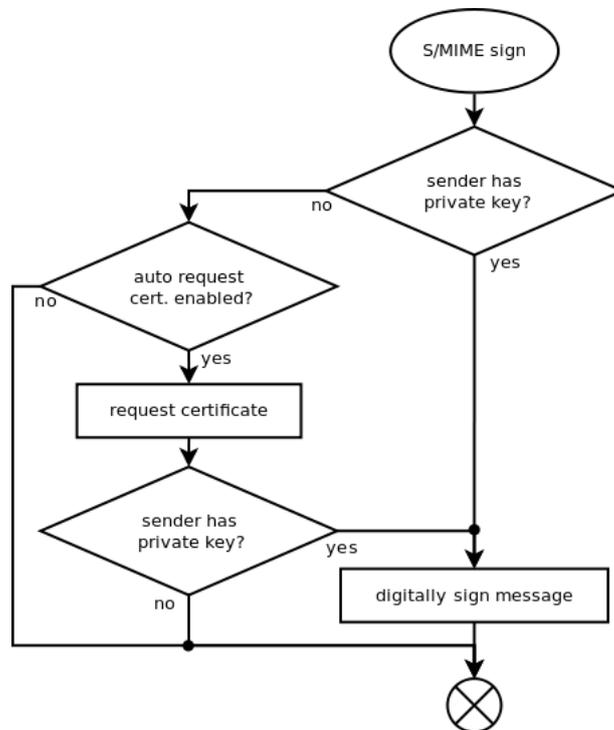


Figure 119: S/MIME sign

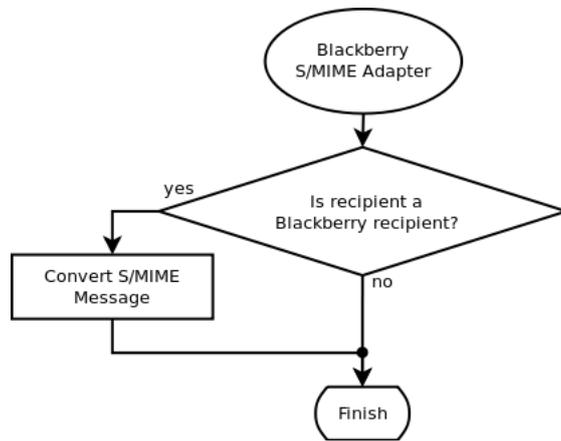


Figure 120: BlackBerry S/MIME adapter

F Comodo certificate request handler

The Comodo certificate request handler requests certificates³¹ from Comodo's Enterprise Public Key Infrastructure (EPKI). Comodo's EPKI is an outsourced Certificate Authority managed by Comodo. The main advantage of using certificates issued by Comodo is that these certificates are by default trusted by most systems (like Windows, Mac OS, Ubuntu).

The Comodo EPKI certificate request procedure is a three step procedure:

1. Apply for certificate.
2. Authorize request.
3. Collect certificate.

After every step, the EPKI manager sends an email to the registered EPKI manager. Because requesting a certificate using the Comodo certificate request handler takes several steps, a certificate is not immediately issued.

The Comodo certificate request handler requires a valid EPKI account. A Comodo EPKI account can be provided by Ciphermail or alternatively directly from Comodo. The following Comodo EPKI account settings can be specified: "Login name", "Login password", "AP", "CA Certificate ID" and "Auto authorize" (see figure 121).

The only required settings are: "Login name", "Login password" and "AP". Step two, "Authorize request", will be done automatically by the Ciphermail gateway when "Auto authorize" is enabled. If "Auto authorize" is not enabled, the authorization step should be done online using the EPKI portal. "CA Certificate ID" should only be specified when the issued certificate should be signed by a non-default CA certificate.

F.1 Tier details

By clicking "view Tier details", Comodo EPKI status information can be retrieved (see figure 122).

G Bulk import

The file format of the file containing all the certificate requests used for the "bulk request" option is as follows:

- The file should be a comma separated file (CSV).
- Values containing commas should be double quoted.
- The first row should contain the column order.

³¹The private key will be generated on the gateway and not leave the gateway. The public key and some identifying information (like email address) will be sent to Comodo. Comodo will then generate, sign and return the certificate.

Comodo Certificate Request Handler settings

The Comodo certificate request handler requires a valid Comodo EPKI account.

view Tier details

Login name
account Username

Login password
account Password

AP
alliance Partner Name

CA Certificate ID
leave blank for default

Auto authorize
automatic authorize certificate requests

Apply Cancel

Figure 121: Comodo EPKI settings

Comodo Tier details

Verification Level: Class 3
Account Status: Active
Reseller Status: Authorized
Web Host Reseller Status:
Epki Status:
Cap Live CCCs:
Peak Live CCCs:
Current Live CCCs:
Authorized Domains:
Error: false
Error Message:

Close

Figure 122: Comodo Tier details

- The CSV is considered to be US-ASCII encoded unless a Byte Ordering Mark (BOM) is used.
- The following columns are supported: "EMAIL", "ORGANISATION", "COMMONNAME", "FIRSTNAME", "LASTNAME"
- "EMAIL" and "COMMONNAME" are mandatory.
- By default, the maximum number of requests in a single CSV file is 10000.
- The maximum length of an individual entry is 256 characters.

Multiple aliases for the columns are available. Column names are case insensitive:

Column	Aliases
EMAIL	email, e
ORGANISATION	organisation, org, o
COMMONNAME	commonname, cn
FIRSTNAME	firstname, fn, givenname, gn
LASTNAME	lastname, ln, surname, sn

G.1 Examples CSV

The following example shows how to import two requests. It uses a combination of column name aliases:

```
"e", "org", "COMMONNAME", "fn", "surname"
"test0@example.com", "organisation 0", "user 0", "first name 0", "last name 0"
"test1@example.com", "organisation 1", "user 1", "first name 1", "last name 1"
```

A similar example but this time the values are not quoted and only the required values email and organisation are specified:

```
e, cn
testA1@example.com, cn1
testA2@example.com, cn2
```