

DJIGZO EMAIL ENCRYPTION

Djigzo for BlackBerry Quick Start Guide



February 24, 2011, Rev: 5459

Introduction

This guide will explain how to setup and configure a Djigzo Virtual Appliance in combination with Djigzo for BlackBerry. This step-by-step guide will be based on an example showing how Djigzo can periodically fetch email from an external Gmail account, encrypt the email and then forward the encrypted email to the BlackBerry's BIS email account.

In This quick start guide we will explain **a)** how to configure the Djigzo gateway to fetch email from an external Gmail account, **b)** create a certificate and private key and import the certificate and private key into a BlackBerry smartphone, **c)** encrypt the email and forward the encrypted email to a BIS email account, **d)** install and configure Djigzo for BlackBerry and finally, **e)** how to configure a Djigzo gateway and Djigzo for BlackBerry, to relay email from a BlackBerry via a Djigzo gateway protected with an encrypted S/MIME tunnel.

Note: This quick start guide uses Gmail as an external store from which email will be forwarded. Email stored on Gmail servers however is not encrypted unless the sender encrypted the message. The use of Gmail in this quick start guide is merely for demo purposes. If all external email should be encrypted, we advise you to run Djigzo as a full SMTP gateway or, other (fully trusted) POP3 servers should be used instead of Gmail.

Running a Djigzo gateway with Fetchmail is not as scalable and reliable as running Djigzo as a full SMTP gateway. If more than a dozen BlackBerry smartphones should be supported by a single gateway, it's better to run Djigzo as a full SMTP gateway. For advanced setups of Djigzo see the Djigzo administration guide for more information.

This guide assumes that the user has a valid Gmail account with POP enabled and a BIS email address on which BlackBerry email can be received.

Note: We advise you to create a new Gmail account for this example. All existing email from the Gmail account will be forwarded to the BlackBerry smartphone when Fetchmail is enabled for the Gmail account. A new Gmail account however is not required, only advised. The Gmail account should not already be configured for a BlackBerry smartphone.

This guide assumes that the following Gmail account and BIS email address are used*:

Gmail account: username: *test@gmail.com*, password: *test*
BIS email: *test@bis.blackberry.net*

* Where needed, the Gmail account and BIS email address used in the examples should be changed to match the real Gmail account and BIS email address.

This guide consists of two parts. The first part explains how to setup Djigzo for BlackBerry for receiving encrypted email. The second part explains how to securely sent email from a BlackBerry smartphone with Djigzo for BlackBerry.

1 Receiving encrypted email

This section explains how to setup a Djigzo gateway server and how to setup Djigzo for BlackBerry for receiving encrypted email. The following steps will be explained:

1. Install Virtual Appliance
2. Enable Fetchmail
3. Login to the Web admin
4. Configure MTA
5. Configure SMTP authentication
6. Configure Fetchmail
7. Create CA
8. Issue certificate
9. Download certificate
10. Configure user
11. Import certificate into BlackBerry
12. Install Djigzo for BlackBerry

1.1 Install Virtual Appliance

Download and install Djigzo Virtual Appliance. The required Virtual Appliance distribution and installation procedure differs between VMware infrastructure (ESX, ESXi etc.) and other VMware virtual machines (VMware player, VMware workstation etc.). For more detailed instructions on how to install the Virtual Appliance see the *Virtual Appliance Guide*.

After the Virtual Appliance has been started, the user must login to the console with the following default credentials:

username: djigzo-admin
password: djigzo

After logging into the Virtual Appliance console, a system configuration tool is started. The system configuration tool will be used to enable Fetchmail.

1.2 Enable Fetchmail

Fetchmail will be used to retrieve email from Gmail by periodically polling the account via POP3. The Djigzo Virtual Appliance has Fetchmail support built-in. Fetchmail however is disabled by default and should therefore be enabled.

Fetchmail can be enabled by opening the menu item **Config**→**Fetchmail...** from the console system configuration tool, select *Enable* and apply (see figure 1).

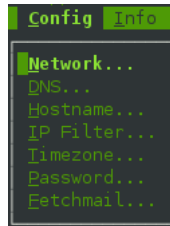


Figure 1: Virtual Appliance config

1.3 Login to the Web admin

Login to the administration page by opening the following URL in a browser: <https://192.168.1.1/>. The actual IP address will be different and should match the IP address of the gateway. The current IP address of the gateway can be retrieved by selecting the menu item **Info**→**Network** from the console system configuration tool.

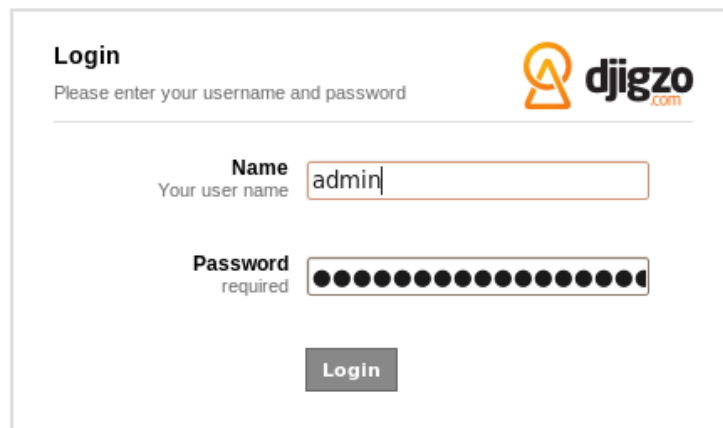
A screenshot of a web browser showing the login page for Djigzo. The page has a white background and a grey border. At the top left, the word 'Login' is displayed in bold. Below it, the text 'Please enter your username and password' is shown. On the top right, there is a logo for 'djigzo.com' which consists of an orange stylized 'A' shape followed by the text 'djigzo.com'. Below the instructions, there are two input fields. The first is labeled 'Name' with the subtext 'Your user name' and contains the text 'admin'. The second is labeled 'Password' with the subtext 'required' and contains a series of black dots. At the bottom center, there is a grey button with the text 'Login' in white.

Figure 2: Login dialog

The login page should appear (See figure 2).

Login credentials: Use the following default credentials:

username: admin
password: admin

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

1.4 Configure MTA

Djigzo should be setup to relay encrypted email via the Gmail *SMTP* servers. The *MTA config* page (see figure 3) can be opened from the Admin menu (**Admin**→**MTA config**).

The following items should be configured:

1. My Hostname
2. External relay host
3. Internal relay host
4. My networks

My Hostname *My Hostname* should be a fully qualified domain name or an IP address. Because in this example all outgoing email will be relayed via Gmail the hostname can be a local name. Use **djigzo.localhost** for the *My Hostname* setting.

Note: if outgoing email should be sent directly (i.e. not relaying email via Gmail) the *My Hostname* should be an externally valid domain name. See the Djigzo administration guide for more information on setting an externally valid *My Hostname*.

External relay host All email to non-relay domains should be relayed via the Gmail *SMTP* server (smtp.gmail.com) via port 587 (this is the mail submission port).

host: smtp.gmail.com
mx: leave unselected
port: 587

Internal relay host All email to relay domains should be relayed via the Gmail *SMTP* server (smtp.gmail.com) via port 587 (this is the mail submission port).

host: smtp.gmail.com
mx: leave unselected
port: 587

MTA config

sasl passwords | MTA raw config

Relay domains

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

Remove

Add domain
Add a new relay domain

Add

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

Remove

Add network
Add a new network

Add

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 3: MTA config

My networks Should be empty unless the gateway is also being used with an external email client (like Outlook, Thunderbird etc.).

The final MTA settings should be similar to the settings seen in figure 3. By pressing the *Apply* button, all changes will be saved and the updated MTA configuration will be reloaded.

1.5 Configure SMTP authentication

All outgoing email will be relayed by the Gmail SMTP servers. Gmail however only allows email to be relayed via the Gmail SMTP servers when the user is authenticated. Enabling authentication requires two steps: *a)* Enable SMTP client authentication, *b)* Add a new SASL account¹.

Enable SMTP client authentication SMTP client authentication is not enabled by default. Gmail requires that all SMTP authentication is protected with SSL.

SMTP client authentication via SSL can be enabled by uncommenting the following lines in the *MTA raw config* page (scroll down the config file and remove the hash [#] in front of the relevant lines):

```
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 *MTA raw config* page can be opened by clicking **Admin**→**MTA config**→**MTA raw config**.

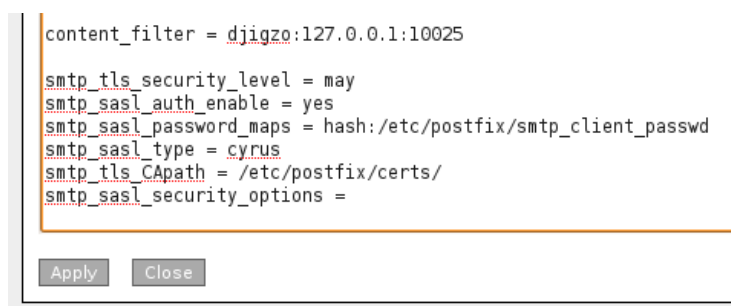


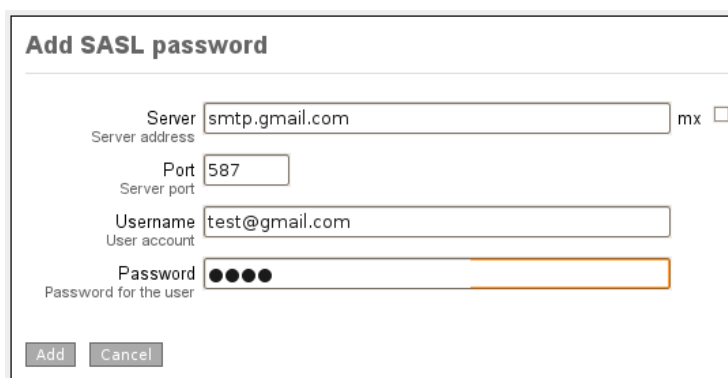
Figure 4: MTA raw config

The final *MTA raw config* should look similar to figure 4. Make sure that all other lines are not modified.

By pressing the *Apply* button, all changes will be saved and the updated MTA configuration will be reloaded.

¹SASL stands for Simple Authentication and Security Layer. This is a framework for authentication and data security in Internet protocols

Add a new SASL account The correct login credentials for the Gmail account should be set. SMTP credentials for a specific host can be added by clicking *sasl passwords* on the *MTA config* page (see figure 3, top-left). A new SASL account should now be added by clicking *add password*. This opens the *Add SASL password* page (see figure 5). Use the following settings:



The screenshot shows a web form titled "Add SASL password". It has four input fields: "Server" (with "smtp.gmail.com" and an "mx" checkbox), "Port" (with "587"), "Username" (with "test@gmail.com"), and "Password" (with four dots). At the bottom are "Add" and "Cancel" buttons.

Figure 5: SASL add password

Server: smtp.gmail.com
Port: 587
Username: test@gmail.com*
Password: test*

* username and password should match the real Gmail account. Note that the username should include *@gmail.com*.

The *Add SASL password* page should look similar to figure 5. The password should now be added by pressing *Add*. The *SASL passwords* page will now be opened (see figure 6) showing all available SASL accounts. By pressing the *Apply* button, all changes will be saved and the updated configuration will be reloaded.

1.6 Configure Fetchmail

Fetchmail will be used to retrieve email from Gmail by periodically polling the account via POP3. The Gmail account to fetch email from and the BIS email address to which encrypted email will be forwarded to should be configured. New accounts from which mail should be fetched can be added with the Fetchmail manager (**Admin**→**Fetchmail manager**).

The following two fetchmail settings should be set: *Postmaster* and *Poll interval*.

Postmaster If email cannot be forwarded, an error message will be sent to the postmaster email address. Set *Postmaster* to an email address on which email can be received. Under normal circumstances email will always be forwarded.

SASL passwords*

add password | delete selected | invert selection

	Server	Port	Mx Lookup	Username	Password
<input type="checkbox"/>	test.example.com	25	false	admin	***

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

Apply Close

Figure 6: SASL passwords

Fetchmail Manager

add account | delete selected | invert selection

	Server	Port	Protocol	Authentication	Username	Pass
<input type="checkbox"/>	pop.gmail.com		Pop3	Password	test@gmail.com	***

Postmaster
email address of the last-resort recipient

Poll interval
background poll interval in seconds

Check certificate
only accept trusted server certificates

Apply Close

Figure 7: Fetchmail manager

In all the examples we will assume the following postmaster email address:

email address: postmaster@example.com*

* The postmaster email address should be changed to match the real postmaster address.

Note: Make sure the Postmaster email address is not the same email address for which email will be fetched to prevent a mail loop.

Poll interval The number of seconds between consecutive checks for new email. The *Poll interval* should not be too low to prevent flooding of the remote server. You are advised to set the *Poll interval* to 30 seconds.

The settings can be saved by clicking *Apply*.

Note: the first time apply is clicked, an error message will be shown (“... no mailservers have been specified.”). This is normal because there are no accounts specified. The error message can be ignored.

Adding new account A new Fetchmail account can be added by clicking *add account* in the Fetchmail manager. The page *Fetchmail Add Account to Poll* will be opened (see figure 8). Email from Gmail will be retrieved with POP3. Use the following settings:

Server: pop.gmail.com
Protocol: Pop3
Authentication: Password
Username: test@gmail.com*
Password: test*
UIDL: should be selected
SSL: should be selected
Forward To: test@bis.blackberry.net*

* username and password should be changed to match the real Gmail account. The username should include *@gmail.com*. The *Forward To* parameter should be the email address of the BIS account on which the BlackBerry receives email.

The new Fetchmail account page should look similar to figure 8. By clicking *Add*, the new Fetchmail account will be added.

Note By applying the new settings Fetchmail will start fetching all existing and new incoming email from the configured Gmail account and forward it to the configured BIS email address. Fetchmail forwarding can be disabled for a specific account by deleting the account from the *Fetchmail manager* and applying the new settings.

Fetchmail will be configured with the new settings and restarted after clicking *Apply* on the Fetchmail manager page (see figure 7).

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 8: Fetchmail manager add account

1.7 Create CA

Djigzo for BlackBerry uses X.509 certificates for encryption and signing of messages. The BlackBerry smartphone therefore requires a certificate and private key to be installed on the BlackBerry smartphone. The Djigzo gateway contains a built-in CA which can be used to create certificates and private keys.

Before a new end-user certificate can be created, a new root and intermediate certificate should be created. Instead of creating new certificates with the built-in CA, existing certificates can be used instead. Instructions on how to use existing certificates however, is beyond the scope of this quick start guide (see the *Djigzo Administration Guide* for more information on using existing certificates).

A new CA can be created by clicking *CA* in the main menu and then select *Create new CA*. This opens the *Create new CA* page (see figure 9). The only required parameters are the *Common name* of the root and intermediate certificate.

The common name of the root certificate should be different from the common name of the intermediate certificate. For example use the companies name prefixed with “root” and “intermediate” respectively as the common name. Leave all other parameters at their default values and click *Create* to create the new root and intermediate certificates. The new CA is now active.

1.8 Issue certificate

The newly created CA can now be used to issue a new end-user certificate (and private key) for the BIS email address. This certificate will be used to encrypt email sent to the BlackBerry BIS email address.

A new certificate can be created with the *Create new end-user certificate* page which can be opened by clicking *CA* in the main menu (see figure 10).

The only two required parameters are: *Email* and *Common name*:

Email: test@bis.blackberry.net*
Common name: Certificate for Djigzo for BlackBerry*

* The *Email* address should be the email address of the BIS account. The common name typically is the users first name and last name.

The new certificate and private key will be created after clicking *Create*.

1.9 Download certificate

The newly created certificate and private key should be imported into the BlackBerry smartphone using the BlackBerry desktop manager. The certificate and private key should therefore be downloaded from the Djigzo gateway and stored in a password protected *.pfx* file.

The certificate and private key can be downloaded by selecting *Certificates* from the main menu. On the *Intermediate and user certificates* page select the end-user certificate with the correct email address (see figure 11). The certificate and private key can be downloaded by clicking *download keys*. A

Certificates	Roots	CRLS	CA	SMS	Settings	Queues	Logs	A
<h3>Create new CA</h3>								
Root certificate								
Validity in days	<input type="text" value="1825"/>							
Key length in bits	<input type="text" value="2048"/>							
Email	<input type="text"/>							
Common name required	<input type="text" value="test root"/>							
<input type="checkbox"/>	more							
Intermediate certificate								
Validity in days	<input type="text" value="1825"/>							
Key length in bits	<input type="text" value="2048"/>							
Email	<input type="text"/>							
Common name required	<input type="text" value="test intermediate"/>							
<input type="checkbox"/>	more							
General								
Make default CA	<input checked="" type="checkbox"/>							
Signature algorithm for certificate signature	<input type="text" value="Sha1 With Rsa"/>							
<input type="button" value="Create"/> <input type="button" value="Close"/>								

Figure 9: Create new CA

Figure 10: New end user certificate

password should now be provided which is used to encrypt the *.pfx* file with. Enter a secure password and click *Download* to start the download process. The *.pfx* file is required during later steps and should be locally stored on the desktop computer.

1.10 Configure user

The Djigzo gateway should be configured in such a way that email is encrypted when email is sent to the BIS email address. A new user object for the BIS email address should therefore be created.

Create a new user object by clicking *Add user* on the left-hand side menu. On the *Adding new user* page, enter the BIS email address and click *Add* (see figure 12).

After the user has been added, the *Edit user* page is opened on which the user preferences for the newly added user can be set. With all settings set to the default gateway settings, only one BlackBerry specific user preference should be changed: *Recipient uses add-on*.

Because this setting is an advanced setting, the *show advanced settings* checkbox should be selected. The *inherit* checkbox for the preference *Recipient uses add-on* should be unchecked and *Recipient uses add-on* should be selected (see figure 13). Any changes to the user preferences should be saved by clicking *Apply*.

Note: The *Recipient uses add-on* setting is required to make sure BIS does not block the S/MIME message.

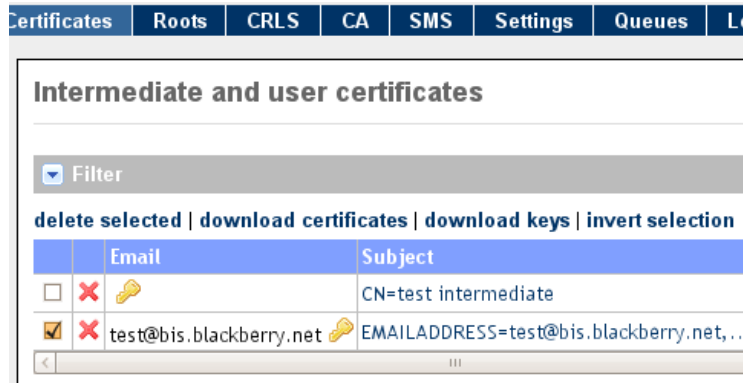


Figure 11: Select end user certificate

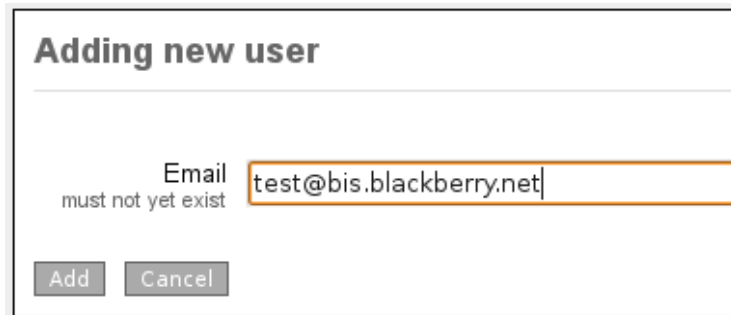


Figure 12: Add new gateway user



Figure 13: Advanced BlackBerry settings

1.11 Import certificate into BlackBerry

The gateway is now correctly setup to start encrypting and forwarding email from the Gmail account to the BlackBerry smartphone. The BlackBerry smartphone however requires a private key for decrypting encrypted messages.

The *.pfx* file created in step 1.9 should now be imported into the BlackBerry smartphone using the BlackBerry Desktop Manager Certificate Synchronization tool (see “Synchronize Certificates” in figure 14). If the Synchronize Certificates option is not available it should be enabled first.

Enable Certificate Synchronization This paragraph can be skipped if the Synchronize Certificates option is already enabled. The Synchronize Certificates option can be enabled by modifying the BlackBerry Desktop Software.

On Windows, open the Control Panel → Add or Remove Programs → Select BlackBerry Desktop Software and click the Change/Remove button. This opens the BlackBerry Desktop Software installation wizard. Enable the “Certificate Synchronization” option and finish the wizard by pressing Next and Finish (see figure 15).



Figure 14: BlackBerry Desktop Manager

Import PFX The *.pfx* file can be imported into the BlackBerry smartphone by connecting the BlackBerry smartphone to the desktop and clicking “Synchronize Certificate” (see figure 14). The first time certificates and keys are synchronized, a new Key Store Password must be set. The Key Store is the store which stores the private keys. The Key Store is password protected. After the password is entered, the Certificate Synchronization tool is started (see figure 16).

To import the *.pfx* file click *Import certificate...* In the *Select Certificate To Import* dialog make sure that “Personal Information Exchange (*.pfx, *.p12)” file type is selected and select the *.pfx* file which was saved on the desktop computer in step 1.9. Click *Open* to import the *.pfx*.

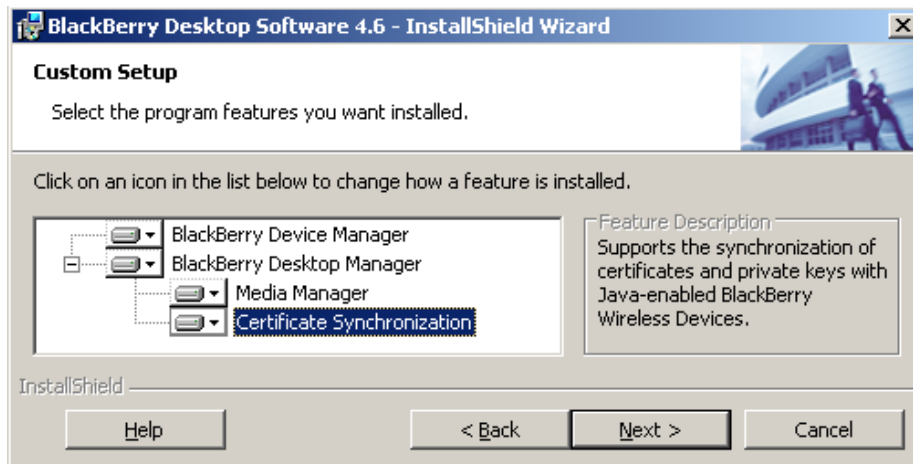


Figure 15: Enable Certificate Synchronization option

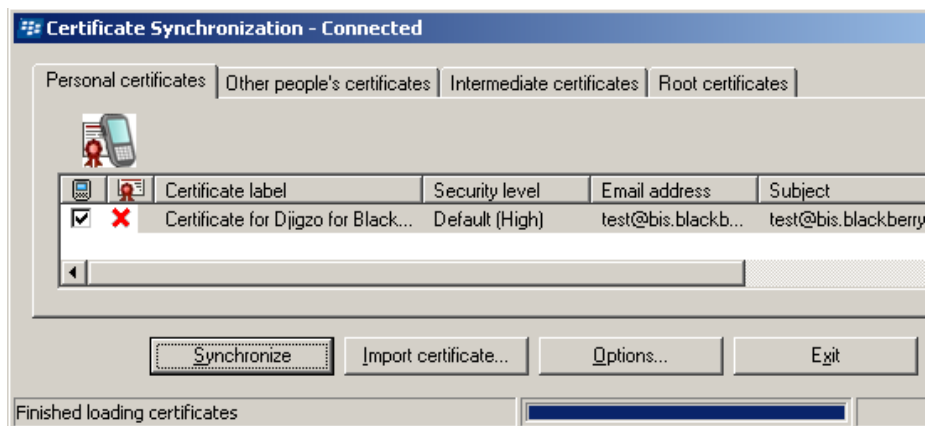


Figure 16: Certificate Synchronization tool

Because the *.pfx* file is password protected the password chosen at step 1.9 must be entered. After entering the password the certificate and private key will be imported into the Windows certificate store. The certificate and private key can now be imported into the BlackBerry smartphone. The certificate and private key are already selected (see figure 16). By clicking *Synchronize*, the selected certificate and private key will be imported into the BlackBerry smartphone.

Note: By default the private key security level will be *High*. This means that the key store password must be entered every time the private key is used to decrypt a message. This is very secure, but not very practical. The private key security level can be modified by opening the certificate synchronization options. See the *Djigzo for BlackBerry Reference Guide* for more information on how to change the security level.

1.12 Install Djigzo for BlackBerry

Djigzo for BlackBerry is a BlackBerry application which should be installed on a BlackBerry smartphone. Djigzo for BlackBerry can be installed over-the-air from <http://m.djigzo.com/bb>. There are different versions for different BlackBerry OS versions: 4.5, 4.6 and ≥ 4.7 .

After Djigzo for BlackBerry has been installed, encrypted email can be received and opened on the BlackBerry smartphone. All email sent to *test@gmail.com* will now be retrieved by Fetchmail, encrypted by the gateway and then forwarded to the address *test@bis.blackberry.net*.

What now follows is a short introduction to Djigzo for BlackBerry. For more detailed information see the *Djigzo for BlackBerry Reference Guide*.

Djigzo for BlackBerry Encrypted email is stored in the inbox of the BlackBerry mail application just like normal non-encrypted email. Whether or not the message is automatically decrypted when the user opens the message depends on the size of the encrypted message.

Messages smaller than 64KB will be automatically decrypted when opened (figure 17 shows an HTML message which was encrypted with 3DES). Messages larger than 64KB are initially not fully delivered to the BlackBerry smartphone. Messages larger than 64KB should be manually opened by the user by selecting *Open Attachment* from the context menu. The message will then be downloaded and opened.

Encrypted messages that should be manually opened can be recognized by the attachment named “attachment.smime” (see figure 18). The body of the message containing the encrypted “attachment.smime” is based on the *BB add-on* template (see the Templates section in the Djigzo Administration Guide for more information).

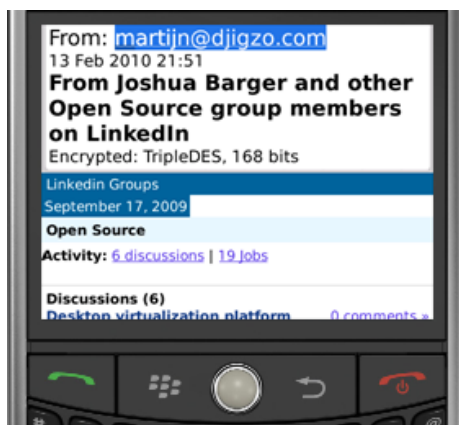


Figure 17: Encrypted HTML message

Key Store password Depending on the selected *Private key security level*, a password must be entered when the message is decrypted (see figure 19).

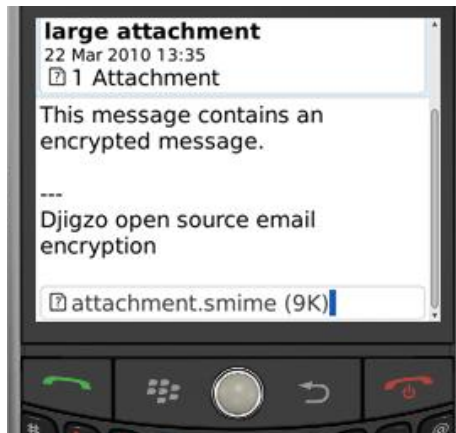


Figure 18: S/MIME attachment

Depending on the settings, the Key Store password will be cached for some time. For more information, see the *synchronization options* section in the *Djigzo for BlackBerry Reference Guide*.

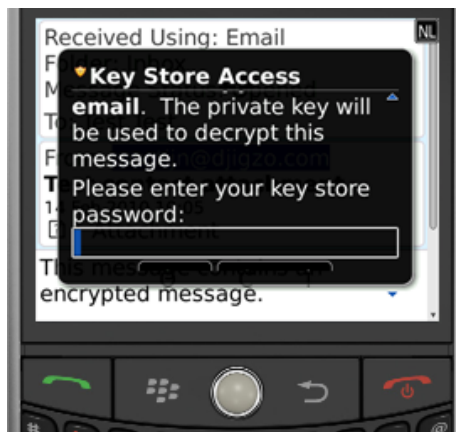


Figure 19: Key Store password

Suitable Private Key not found If a message is encrypted, but the BlackBerry smartphone cannot find the correct private key to decrypt the message with, a warning message will be shown. For more information on how to find out which certificates were used for encryption, see the *Djigzo for BlackBerry Reference Guide*.

Attachments Encrypted messages can contain attachments. The complete message, including any attachment, is encrypted. Djigzo for BlackBerry allows attachments to be opened and saved. Only attachments for which a content handler is registered can be opened (for example .doc and .xlt files will be opened with *Documents to Go*). Attachments are shown at the bottom of the email (see

figure 20). Attachments can be opened by clicking the attachment. Attachments can be saved by selecting the attachment and selecting *Save Attachment* from the context menu. A save-as popup screen will be opened (see figure 21).

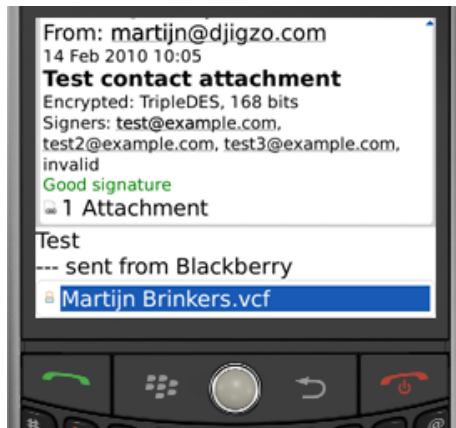


Figure 20: Message with attachment and Good signature.

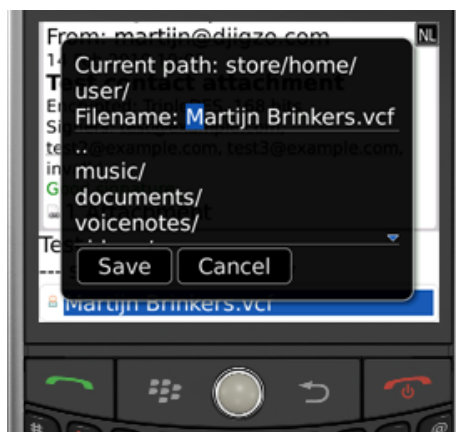


Figure 21: Save attachment

Finish

Now Djigzo for BlackBerry has been installed and the gateway has been configured, encrypted email can be received and opened on the BlackBerry smartphone. All email sent to *test@gmail.com* will now be retrieved by Fetchmail, encrypted by the gateway and then forwarded to the address *test@bis.blackberry.net*.

Email sent to *test@gmail.com* which is already S/MIME encrypted (for example encrypted with Outlook) can be opened by Djigzo for BlackBerry as long as the BlackBerry smartphone contains the correct private key to decrypt the message with.

The next section will explain how email sent with Djigzo for BlackBerry can

be securely relayed via an encrypted S/MIME tunnel to the Djigzo gateway². This section can be skipped if sending email with Djigzo for BlackBerry is not required.

2 Sending secure email

This section explains how to send secure email from a BlackBerry smartphone with Djigzo for BlackBerry. The most difficult part of email encryption is key management. Selecting the correct certificate for a recipient, importing root certificates etc. requires some knowledge of the PKI process. This is especially hard on mobile devices. Djigzo for BlackBerry therefore relies on the Djigzo gateway for most certificate management functions.

Messages sent from a BlackBerry smartphone with Djigzo for BlackBerry are encrypted with a server certificate and digitally signed with a certificate from the BlackBerry's key store. The message is then sent to the Djigzo gateway by email via a signed and encrypted S/MIME tunnel. The gateway checks whether the sender is allowed to relay messages through the gateway and whether the digital signature is correct. Only if the signature is correct and the message is signed with the correct private key, will the message be forwarded to the final recipients (see figure 22). It depends on the gateway settings whether or not messages sent to the final recipients are encrypted by the Djigzo gateway.

Messages sent from the BlackBerry smartphone will be relayed by the gateway to the final recipients. The gateway therefore has to handle relay messages differently from 'normal' messages. In this example the Djigzo gateway is not setup as a full SMTP server. Email is therefore not directly received but fetched with fetchmail. Another Gmail account should therefore be used for email that should be relayed.

Note: We advise you to create a new Gmail account for the relay email address. All existing email on the Gmail account will be forwarded to the Djigzo gateway when Fetchmail is enabled. A new Gmail account however is not required, only advised. The only requirement is that the relay Gmail account is not the same Gmail account as the Gmail account used in the *Receiving encrypted email* section and that the Gmail account is not already setup for the BlackBerry smartphone.

In this example the following relay account will be used*:

```
username: relay@gmail.com  
password: test
```

* Where needed, the Gmail account used in the examples should be changed to match the real Gmail account.

Note: only one relay account is required for multiple users. The relay account is only used to temporarily store the relay messages until the messages are

²With an S/MIME tunnel, every message is S/MIME encrypted. This is different from a TLS tunnel where only the communication channel is encrypted but not the individual messages.

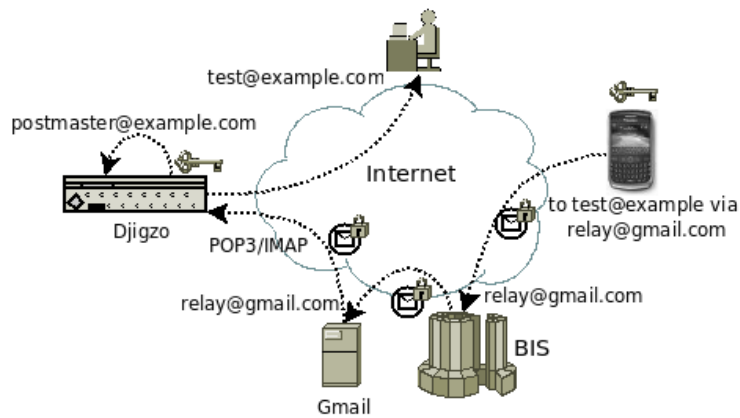


Figure 22: BlackBerry user sends a message. The message is S/MIME signed and encrypted (secure enveloped) and sent to relay@gmail.com. The Djigzo server fetches the email via POP3, decrypts it and sends it to test@example.com

fetches by the gateway.

To setup an authenticated S/MIME tunnel between the gateway and Djigzo for BlackBerry the following steps are required:

1. Configure Fetchmail account
2. Configure Djigzo for BlackBerry for relay
3. Configure gateway user for relay

2.1 Configure Fetchmail account

Email securely sent with Djigzo for BlackBerry is delivered to the relay email address where it will be picked-up by the Djigzo gateway for further delivery. Because the Djigzo gateway is not setup as a full SMTP server, fetchmail should be configured to periodically retrieve new email from the relay account. Adding a new Fetchmail account is already explained on page 8.

Use the following settings for the new relay fetchmail account:

Server: pop.gmail.com
Protocol: Pop3
Authentication: Password
Username: relay@gmail.com*
Password: test*
UIDL: should be checked
SSL: should be checked
Forward To: the postmaster email address. See postmaster on page 8

* username and password should be changed to match the real Gmail account. The username should include @gmail.com.

Forward To The *Forward To* parameter should be the email address of the postmaster (this should be the same as the postmaster email address used on page 8). Normally when everything is setup correctly will the Djigzo gateway relay the email to the final recipient.

However, if the sender is not allowed to relay (see *Relay allowed* on page 26) or if the message is not signed with an approved signing certificate for the sender (see *Select relay certificate* on page 26) the message will not be relayed and the message will be sent to the *Forward To* address. Make sure the *Forward To* address is not equal to the relay email address (to prevent a mail loop).

2.2 Configure Djigzo for BlackBerry for relay

Email sent with Djigzo for BlackBerry is protected with an authenticated and encrypted S/MIME tunnel. The message is relayed by the Djigzo gateway to the final recipients (see figure 22). Because the message will be relayed by the Djigzo gateway, the message should be encrypted with a certificate for which the gateway has a private key. To make sure only approved senders are allowed to relay messages via the gateway, messages should be signed with a private key.

The following Djigzo for BlackBerry settings must be configured: *From*, *Sign cert*, *Enc. cert* and *Relay email*. If one of these settings is missing the message cannot be sent and a warning will be shown. The configuration screen can be opened by clicking the Djigzo icon in the download folder³ (see figure 23).



Figure 23: Djigzo Settings Icon

From When a relay message is forwarded by the gateway, the *From* header of the new message will be set to this value. Set the from header to the BIS email address *test@bis.blackberry.net*. This should be the same email address as the email address of the newly added user from step 1.10.

Signing certificate (*Sign cert*) The signing certificate is the certificate which is used for digitally signing outgoing messages and is used to authenticate

³By default, newly installed applications are stored in the download folder.

the sender of the message. A signing certificate can be selected by pressing the “...” button. Select the certificate that was previously imported (see figure 24).



Figure 24: Select signing certificate

Encryption certificate (*Enc. cert*) Email sent from the BlackBerry smartphone must be encrypted with a certificate for which the Djigzo gateway has a private key (the Djigzo gateway should be able to decrypt the message). The Encryption certificate will be used to encrypt all email sent from the BlackBerry smartphone (via an S/MIME tunnel). An encryption certificate can be selected by pressing the “...” button. There are multiple certificates to choose from. Select the certificate that was previously imported (see figure 25).



Figure 25: Select encryption certificate

Relay email When sending encrypted email with Djigzo for BlackBerry, the email is securely relayed by the Djigzo gateway via an encrypted S/MIME tunnel. The *Relay email* address should be set to the email address of the relay Gmail account:

email address: relay@gmail.com*

* change the email address to match the real relay address.

2.3 Configure gateway user for relay

When sending encrypted email with Djigzo for BlackBerry, email is securely relayed by the Djigzo gateway via an encrypted S/MIME tunnel. The Djigzo gateway decrypts the message, checks whether the sender is allowed to relay via the Djigzo gateway and delivers the message to the final recipient. The Djigzo gateway should therefore handle relay emails differently from ‘normal’ emails (see the introduction of *Sending secure email* on page 21).

To make a distinction between relay and non-relay messages, the gateway needs to know which email address is used for the relay messages. The *Relay email address* setting is a special email address on which the Djigzo gateway listens for incoming relay messages.

A message will only be relayed if the sender is allowed to relay and if the message is signed with an approved certificate. The relay email address and the user relay settings should be setup with the Djigzo Web admin.

Relay email address The relay email address is the email address the gateway listens on for relay messages sent from a BlackBerry with Djigzo for BlackBerry. The relay email address should be specified on the advanced relay global settings page (see figure 26). The global settings page can be opened by clicking *Settings* from the menu (the relay setting is an advanced setting so *show advanced settings* should be checked).

Because all email retrieved with fetchmail from the relay Gmail account is forwarded to the “postmaster” email address (see *Configure Fetchmail Account* on page 22) the *Relay email* address of the gateway should be set to the “postmaster” email address*.

* change the email address to match the real postmaster address.

Setting	Value	Inherit
Relay allowed	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Relay validity interval	7200 (min)	<input checked="" type="checkbox"/>
Bounce mode	Never	<input checked="" type="checkbox"/>
Relay email	postmaster@example.com	<input type="checkbox"/>

Figure 26: Global Relay Settings

Relay allowed A sending user is only allowed to relay email if *Relay allowed* is selected. By checking the global *Relay allowed* setting all senders are allowed to relay. The sending user still requires an approved signing certificate for relaying. Clicking *Apply* saves the current changes.

Note: If a relay message is received by the gateway but the sender is not allowed to relay, the message will be delivered to the *Forward To* email address (which is set to the postmaster address in these examples).

Make the postmaster an internal recipient All relay email is forwarded to the “postmaster” address (see *Configure Fetchmail Account* on page 22). Email sent to this email address is checked by the gateway to see if the email is a relay message sent with Djigzo for BlackBerry. The gateway only checks whether the email is a relay email if the *Relay email address* is an internal address. The “postmaster” user should therefore be added as an internal user (see figure 27).



Figure 27: Postmaster should be an internal user

Select relay certificate for the BIS address The Djigzo gateway checks whether the relay message sent by Djigzo for BlackBerry is signed with an approved signing certificate. If the message is not signed with an approved certificate, the message will not be relayed and will be sent to the *Forward To* email address (which should be set to the postmaster email address).

Because email sent from the BlackBerry smartphone with Djigzo for BlackBerry is sent by user `test@bis.blackberry.net` the relay certificates for this user should be set to allow email to be relayed.

The relay certificates for user `test@bis.blackberry.net` can be set by clicking the user in the user overview (this is the user that was added in in section 1.10) and selecting the advanced settings. Make sure that *Relay allowed* is checked.

Now click on *Select relay certificates* (see figure 28). The *Select relay certificates* page will be opened (see figure 29). Select the certificate for email address `test@bis.blackberry.net` (this is the certificate which was created in section 1.8 *Issue certificate*).

Save the settings by clicking *Apply*.

Relay

Relay allowed inherit

Relay validity interval (min) inherit

Bounce mode inherit

Relay certificates [select relay certificates](#)

Figure 28: Advanced settings: relay certificates for user test@bis.blackberry.net

Select relay certificates for user test@bis.blackberry.net

[back to test@bis.blackberry.net](#)

Filter

Filter by no filter email subject issuer

Allow expired missing key alias

Email	Subject	Expired	Not B
<input checked="" type="checkbox"/> test@bis.blackberry.net	EMAILADDRESS=test@bis.blackberry.net, ...	No	Mar 1

Figure 29: Select relay certificates

Finish

It should now be possible to securely send messages from the BlackBerry with Djigzo for BlackBerry. Email sent with Djigzo for BlackBerry will be S/MIME encrypted, signed and sent to relay@gmail.com, the Djigzo gateway will then check the signature and forward the message to the final recipient(s).

Note: if a message was not correctly relayed, the MPA log (Logs→MPA) will provide more information as to why the message was not relayed.

Final note

In this quick start guide, we showed you how to forward email from a Gmail account to a BlackBerry smartphone in a secure - encrypted - way. We also showed you how email sent from a BlackBerry with Djigzo for BlackBerry can be relayed via a Djigzo gateway.

Alternatively, Djigzo can be setup as a full SMTP gateway. Running Djigzo as a full SMTP gateway is more scalable, more secure and easier to manage. For advanced setups of Djigzo (like running Djigzo as a full SMTP gateway) see the Djigzo administration guide for more information.