

DJIGZO EMAIL ENCRYPTION

---

# Djigzo white paper

---



*Author:* Martijn BRINKERS

May 3, 2010, Rev: 4193



## Introduction

Most email is sent as plain text. This means that anyone who can intercept email messages, either in transit or at rest, can read the content. Today, companies and governments realize that this is unacceptable. Email needs to be confidential, email needs to be encrypted.

Djigzo offers open source products that help to automatically secure email and protect against unauthorized access of email in transit and at rest.

Djigzo Email Encryption Gateway is a standards based centrally managed email server (MTA) that encrypts and decrypts your incoming and outgoing email at the gateway level. Because Djigzo Email Encryption Gateway functions as a general SMTP email server, it is compatible with any existing email infrastructure like Microsoft Exchange. Djigzo Email Encryption Gateway can be run stand-alone or as a VMware Virtual Appliance.

Djigzo for BlackBerry<sup>®</sup> is an add-on to the Djigzo Email Encryption Gateway which can be used to send and receive S/MIME digitally signed and encrypted email from a BlackBerry<sup>®</sup> smartphone.

## Djigzo Email Encryption Gateway

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

Djigzo currently supports two encryption standards: S/MIME and PDF encryption. S/MIME provides authentication, message integrity and non-repudiation (using X.509 certificates) and protection against message interception. S/MIME uses public key encryption (PKI) for encryption and signing. Email that is encrypted and/or digitally signed by Djigzo can be read in Outlook, Thunderbird and other mail clients, provided the user has the proper email certificates installed.

Despite the fact that products like Djigzo makes S/MIME fairly easy to use, some recipients might find S/MIME encryption too cumbersome. Especially when you only need to exchange secure email once, or a few times over a longer period, installing an S/MIME certificate might be more problematic than it's worth. To accommodate for those situations we have included a PDF encryption module in Djigzo. You can configure Djigzo to automatically convert outgoing email to a PDF file and encrypt it using standard PDF encryption techniques. The receiver needs a password to decrypt, which you can provide them by using the built-in Short Text Service (SMS) in Djigzo or alternatively the password can be sent back to the sender of the message (the sender is then responsible for

**“Djigzo is compatible with any existing email infrastructure like Microsoft Exchange and Lotus Domino”**

delivering the passwords to the recipients). A password can be automatically generated or manually set. By using a separate channel for sending passwords, PDF encryption is almost as secure as full S/MIME encryption (provided that the password is long enough to withstand a brute force attack). PDF encryption in Djigzo is intuitive and easy. There's no need to specifically instruct end-users.

Djigzo is compatible with any existing CA server (like EJBCA or Microsoft CA) and with certificates from external commercial and non commercial CA providers (for example Verisign, Comodo and CACert). Alternatively, Djigzo contains a basic Certificate Authority (CA) which allows you to create certificates for internal and external users. Certificates can be transported to external recipients in a password protected format. The password can be automatically generated and provided to the recipient as a Short Text Service (SMS). Installation of the certificate in the recipients mail client is straightforward. This allows you to setup your own private PKI with external recipients.

## General features

- Virtually unlimited number of users and certificates.
- Sender notification after email encryption.
- Settings can set at global, domain or user level.
- Automatic backup to remote share at set intervals.
- Web based interface.
- Separate back-(encryption engine) and front-end (SOAP API).
- Tightly integrates with Postfix (MTA).
- Java, Spring based. Services can be easily replaced and/or extended.
- GPLv3 licensed (commercial licensing available).
- Packages available for Ubuntu, Debian, RedHat/Centos.
- Ready-to-run VMware Virtual Appliance for ESX/ESXi and VMware workstation/player available.
- TAR distribution available for other systems that support Java and Postfix.

## S/MIME features

- S/MIME 3.1 (X.509, RFC 3280).
- Built-in CA which can be used to securely issue certificates for internal and external users.
- Automatic and manual certificate selection.
- Domain certificates (encryption to domains with just one certificate).
- Certificates are automatically extracted from incoming email.
- Support for multiple certificates per sender/recipient.

- Incoming email is automatically decrypted.
- Immune against 'corruption' by non S/MIME aware disclaimer services.
- Certificate revocation lists (CRLs) are automatically downloaded (LDAP and HTTP).
- Certificate trust lists (CTLs) can be used to black or white-list certificates.
- Compatible with existing S/MIME implementations (Outlook, Lotus Notes, Thunderbird etc.).
- S/MIME support for Blackberry BIS users with Blackberry add-on.
- Optional support for Hardware Security Modules (HSM).

### **PDF email encryption features**

- Email is automatically converted to an encrypted PDF (including all attachments).
- PDF is encrypted with AES-128.
- PDF passwords can be automatically generated per user and sent by SMS.
- The recipient can reply with the built-in secure portal.

## Djigzo Email Encryption Gateway with content/virus scanners

A content scanner can be used in combination with Djigzo Email Encryption 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 1.

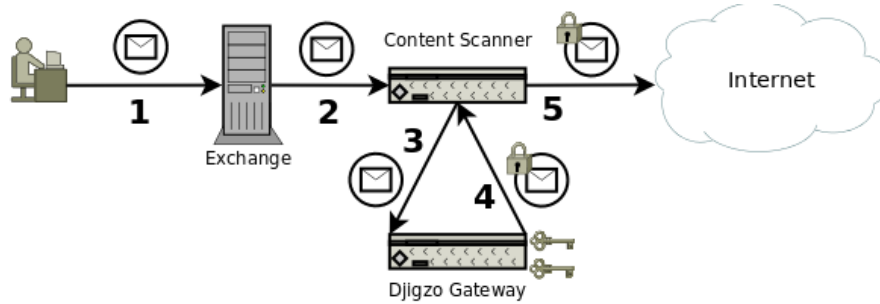


Figure 1: Content scanning

### Djigzo 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. Djigzo 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 2.

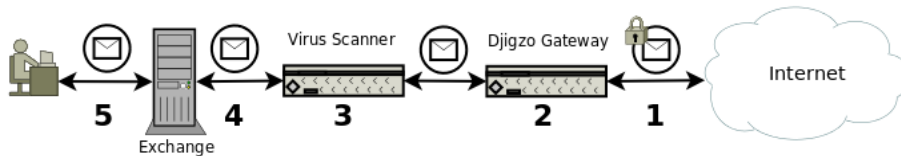


Figure 2: Virus scanning

### Djigzo with virus scanning:

1. S/MIME encrypted message is received from the Internet.

2. Djigzo 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 2 shows how encrypted outgoing email can be virus scanned.

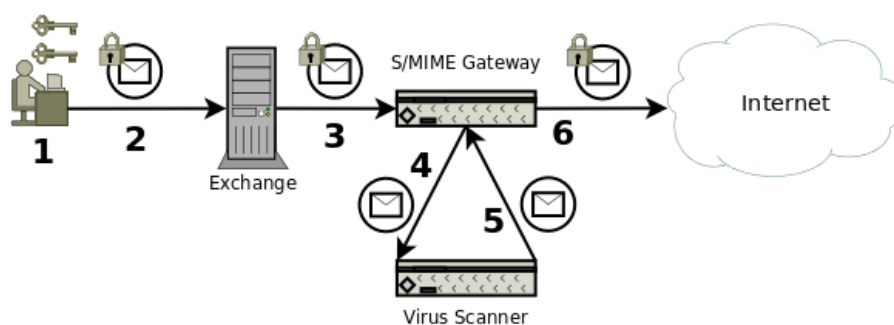


Figure 3: Virus scanning with desktop encryption

**Djigzo 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 Djigzo gateway.
4. Djigzo 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 Djigzo gateway.
6. The Djigzo gateway re-encrypts the message and sends the message to the external recipient.

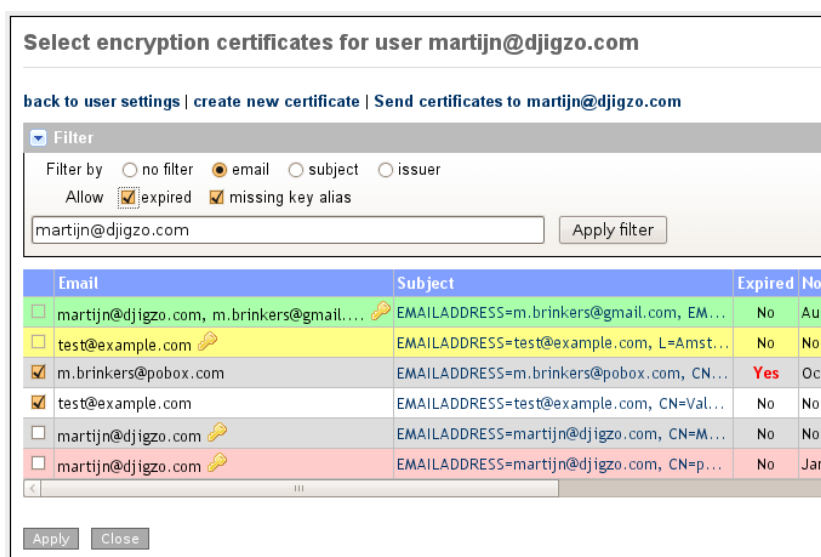


Figure 4: Select encryption certificates

## S/MIME

S/MIME is based on *Public Key Infrastructure* (PKI) and uses X.509 certificates. 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. S/MIME uses a hierarchical trust model. 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).

Because trust is inferred from other entities it should be 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 issuer's 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. Most email clients, like Outlook and Lotus Notes, support S/MIME out of the box.

**“S/MIME is supported by most email clients.”**

When required, Djigzo will automatically select the correct certificates for signing and encryption based on strict PKI rules. Only certificates that are valid (i.e. trusted, not expired, not revoked) are automatically used (see figure 4)

## PDF encryption

PDF encryption can be used as a light-weight alternative to S/MIME encryption. PDF allows you to decrypt and read encrypted PDF documents. The basic idea of Djigzo PDF email encryption is that the complete message, including all attachments, sent by a user is converted to a password encrypted PDF document<sup>1</sup>. The complete document, i.e. the body and all attachments, is encrypted. A standard message, with the encrypted PDF attached, is then sent to the recipient. The recipient can open the PDF by entering the password.

**“PDF encryption in Djigzo is intuitive and easy. There’s no need to specifically instruct end-users.”**

There are various ways the password used to encrypt the PDF with can be set. The password can be statically set by the administrator, the password can be randomly generated and delivered to the recipient via a Short Text message<sup>2</sup> (SMS) or the password can be randomly generated and sent back to the message originator (who should then securely deliver the password to the recipient). A PDF encrypted message looks similar to figure 5. All email clients, including webmail like Gmail, Hotmail etc. are supported. The message contains a general text body which is based on a configurable template. The encrypted PDF is attached to the message. The PDF can be opened with any PDF reader.



Figure 5: Message with encrypted PDF

<sup>1</sup>The PDF is encrypted with AES-128

<sup>2</sup>Using the built-in SMS gateway

After decryption, the PDF will be opened by the default PDF reader. The PDF will be shown as an email message. All attachments can be accessed from the attachment pane (see figure 6). The recipient can securely reply to the encrypted PDF by clicking the reply link in the PDF.

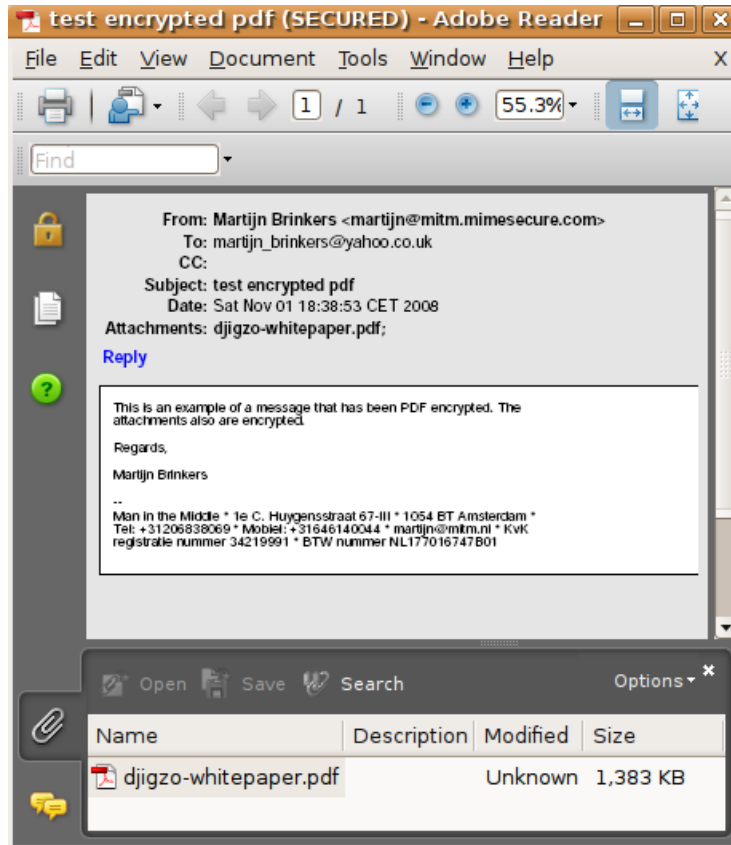


Figure 6: PDF decrypted message. Attachments can be opened from the attachment pane. The recipient can securely reply by clicking the *Reply* link.

## Djigzo for BlackBerry

The BlackBerry® smartphone is the most secure generally available smartphone on the market. All communication between a BlackBerry Enterprise Server (BES) and a BlackBerry smartphone is encrypted with 3DES or AES. For added security the S/MIME support package can be installed allowing email to be digitally signed and encrypted using digital certificates. BlackBerry Internet Service (BIS) users however, do not have the same level of protection that BES users have.

Even though all communication between the carriers BIS and a BlackBerry smartphone is encrypted, data from the carriers BIS to the Internet is not. Email sent to and from a BlackBerry smartphone goes without any protection and can potentially be intercepted and/or modified by any intermediate gateway. It is unfortunate that even though the BlackBerry smartphone has built-in functionality to handle S/MIME encrypted email, the S/MIME support package is not supported by BIS.

**“With Djigzo for BlackBerry, all email on the BlackBerry is S/MIME encrypted.”**

Djigzo for BlackBerry is an add-on to the Djigzo Email Encryption Gateway which can be used to send and receive S/MIME digitally signed and encrypted email from a BlackBerry smartphone. Djigzo for BlackBerry is used in combination with the Djigzo Email Encryption Gateway. Djigzo for BlackBerry integrates with the built-in BlackBerry mail application.

### Features

- S/MIME encryption and digital signing using X.509 certificates.
- Compatible with BIS.
- Is compatible with existing S/MIME clients (like Outlook and Lotus Notes).
- Message body and attachments are encrypted.
- HTML email support.
- Uses BlackBerry encryption functionality (3DES, AES, X.509, S/MIME).
- Uses the BlackBerry built-in key and certificate store.
- Is compatible with the BlackBerry smart card reader.
- Encrypted messages sent from BlackBerry smartphone are securely relayed by the Djigzo gateway via an encrypted S/MIME tunnel.
- Because email is relayed by the Djigzo gateway, email sent from the BlackBerry can be easily archived using any existing email archiving functionality.
- Messages are stored on the BlackBerry smartphone in encrypted form.
- Because email is relayed by the Djigzo gateway, all email originates from the companies IP range. This is especially useful when the companies domains have SPF records setup.

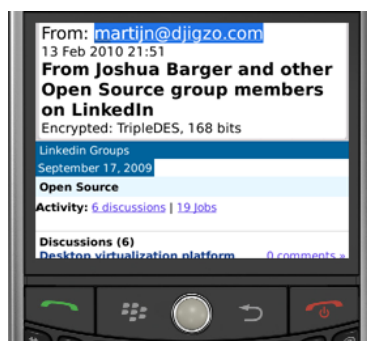


Figure 7: BlackBerry S/MIME encrypted HTML message.

---

## Contact information

Martijn Brinkers  
martijn@djigzo.com  
1e Constantijn Huygensstraat 67-III  
1054 BT Amsterdam  
The Netherlands  
**T:** +31 858782872  
**M:** +31 611346981

---

The Trademark BlackBerry<sup>®</sup> is owned by Research In Motion Limited and is registered in the United States and may be pending or registered in other countries. Djigzo is not endorsed, sponsored, affiliated with or otherwise authorized by Research In Motion Limited.