

Djigzo white paper

Why should you encrypt your email?

Most email is sent as plain text. This means that anyone who can intercept email messages, can read and change the content without you noticing. Today, companies and governments realize that this is unacceptable. Email needs to be confidential. Email needs to be encrypted.

Djigzo email encryption gateway is an email server (MTA) that encrypts and decrypts your incoming and outgoing email. Because Djigzo serves as a general SMTP email server, it is compatible with any existing email infrastructure and can easily be placed before or after existing email servers. 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. 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 is so easy from an end-users perspective that the end-user requires no additional learning.

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.

Djigzo 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.
- Multiple administrator roles supported.
- Separate back-end (encryption engine) and front-end (Web based, SOAP-API)
- Tightly integrates with Postfix (MTA)
- Built-in SMS gateway.
- Java, Spring based. Services can be easily replaced and/or extended.
- Can be installed stand-alone or as a "Virtual appliance".
- Proxy support.
- Open Source licensed (AGPLv3). Non-open source licensing available upon request.

S/MIME features

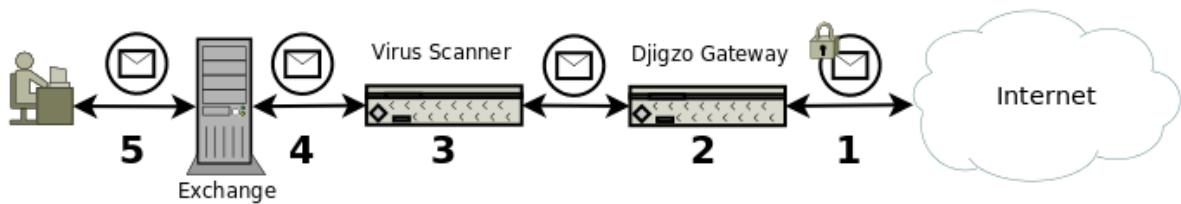
- S/MIME 3.1 (X.509, RFC 3280).
- Built-in CA which can be used to issue certificate for internal and external users.
- Automatic and manual certificate selection.
- Configurable keyword or header can trigger encryption and/or signing.
- Domain certificates (encryption to certain domains with just one 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).
- Compatible with existing S/MIME implementations (Outlook, Outlook express, Lotus Notes, BlackBerry etc.)
- S/MIME support for BlackBerry BIS users with optional Djigzo 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 Short Text Message (SMS)
- The recipient can securely reply to the PDF via the built-in secure portal.

Infrastructure

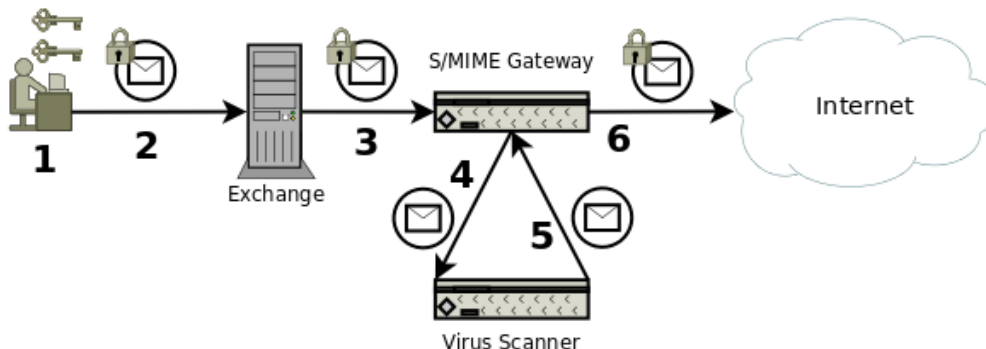
The most typical setup is to install Djigzo as a store-and-forward email server between the Internet and the virus scanner (see Figure 1: Djigzo with Virus Scanner).



- 1) S/MIME encrypted message is received from the Internet
- 2) Djigzo decrypts the message
- 3) The decrypted message (possibly signed) is scanned for viruses
- 4) After virus scanning the message is forwarded to Exchange
- 5) User reads the message (and checks the signature if the message was signed)

Figure 1: Djigzo with Virus Scanner

With full end-to-end encryption (ie. encryption/decryption on the desktop) it's impossible to scan the incoming email for viruses at the gateway level because the virus scanner cannot read the encrypted message. If gateway level scanning is required and a weaker form of end-to-end encryption is acceptable email can be decrypted by the Djigzo server prior to virus scanning and re-encrypted after virus scanning (see Figure 2: Djigzo with Virus Scanning end-to-end).

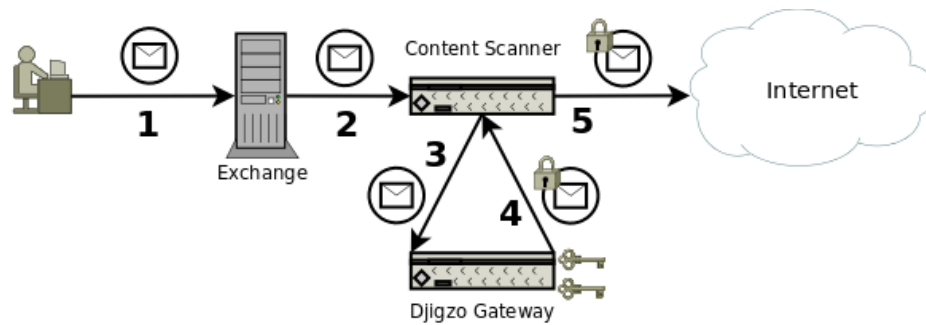


- 1) User encrypts message with personal certificate and receivers certificate
- 2) S/MIME encrypted message is sent to Exchange
- 3) Exchange sends S/MIME encrypted message to S/MIME Gateway
- 4) S/MIME Gateway decrypts message with senders private key and sends decrypted message to Virus Scanner
- 5) Virus Scanner scans message and if clean sends it back to S/MIME Gateway
- 6) S/MIME Gateway re-encrypts the message and sends the message to the recipient

Figure 2: Djigzo with Virus Scanning end-to-end

Because email is decrypted by the Djigzo gateway it's no longer full end-to-end encryption. However, the email is still stored in encrypted form on the Exchange server.

Djigzo can also be integrated with any existing content scanner (see Figure 3: Djigzo with Content Scanner). This allows you to force encryption based on message content (for example when the message contains a Social Security Number)



- 1) User sends unencrypted message
- 2) Exchange forwards message to Content Scanner
- 3) Content Scanner detects that the message must be encrypted (for example a SSN)
- 4) Djigzo Gateway encrypts the message (with S/MIME or PDF)
- 5) Content Scanner sends the encrypted message to the Internet

Figure 3: Djigzo with Content Scanner

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. Attachments added to the PDF are also encrypted.

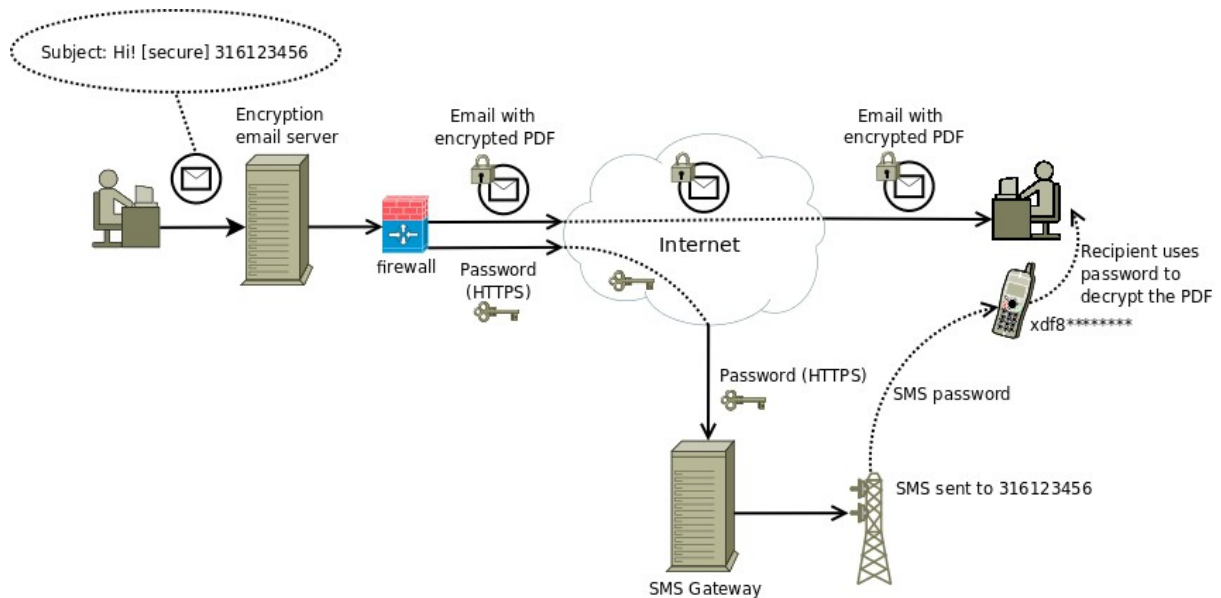


Figure 4: PDF encryption

The basic idea of Djigzo PDF email encryption is that the message sent by the user is converted to a password encrypted PDF¹ (including all attachments). A standard message is sent to the recipient containing the encrypted PDF. The recipient can open the PDF by entering the password. The password for the PDF can be set by the administrator or a password can be randomly generated for each message and sent to the recipient via a Short Text message (SMS) with the built-in SMS gateway.

¹The PDF is encrypted with AES-128

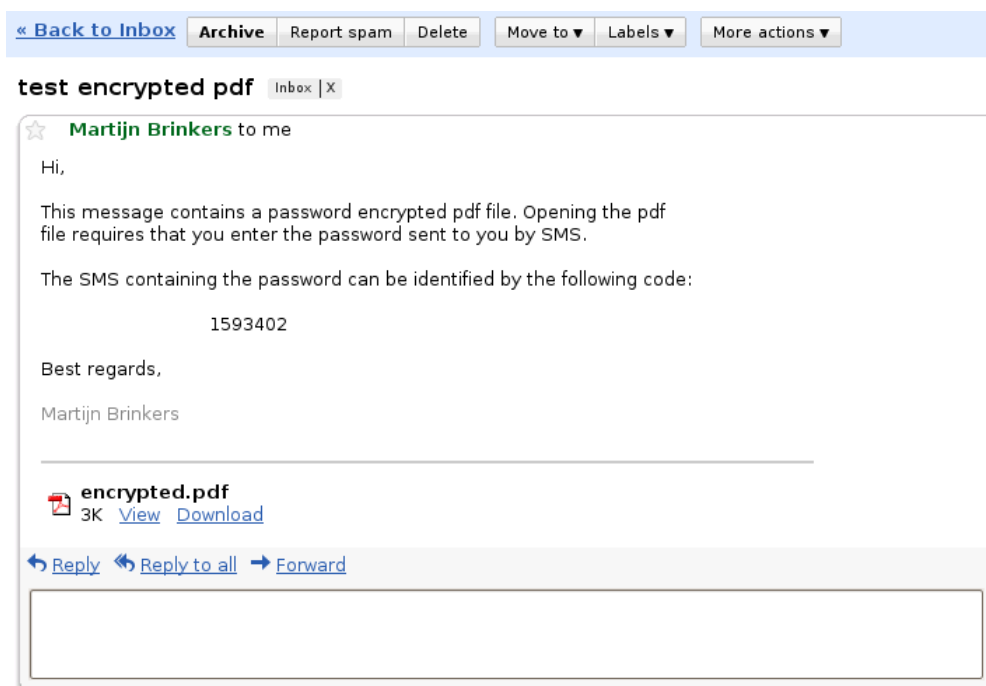


Figure 5: PDF encrypted message

The recipient can securely reply to the encrypted PDF by clicking the reply link in the PDF. Djigzo can be setup to allow senders to specify the recipient's telephone number for the Short Text message (see Figure 4: PDF encryption).

A PDF encrypted message looks similar to Figure 5: PDF encrypted message. All email clients, including webmail like Gmail, Hotmail etc. are supported. The message contains a general message body (based on a configurable template) and the encrypted PDF. The PDF can be opened with any PDF reader. The PDF reader asks for the password. If the correct password is entered the message including any attachment will be shown (see Figure 6: Encrypted PDF).

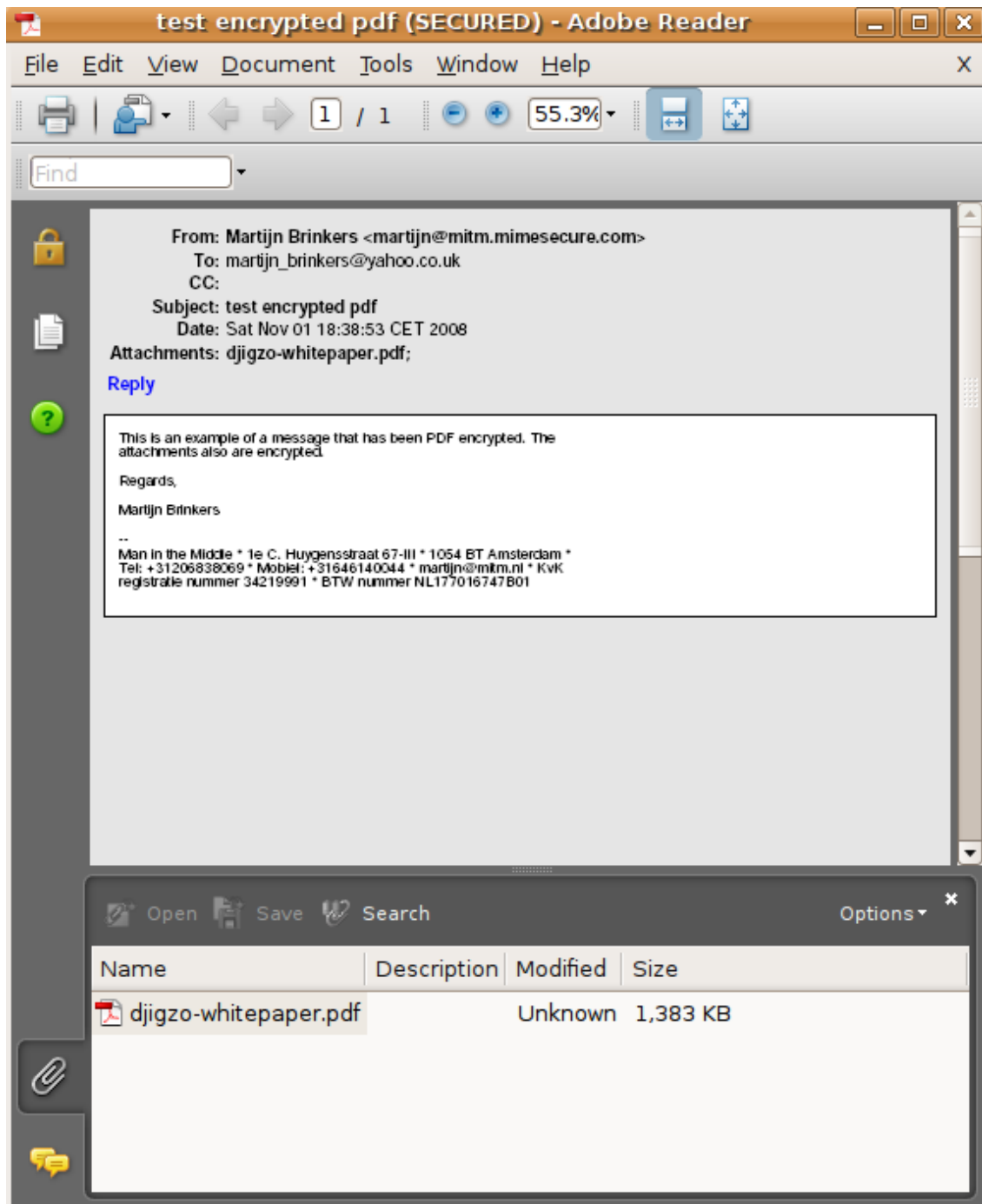


Figure 6: Encrypted PDF

For more detailed information download the Djigzo administration and setup guides from our website

Contact information

Martijn Brinkers

martijn@djigzo.com

1^e Constantijn Huygensstraat 67-III

1054 BT Amsterdam

The Netherlands

+31611346981