CIPHERMAIL EMAIL ENCRYPTION

# Ciphermail S/MIME Setup Guide



April 4, 2016, Rev: 6882

Copyright © 2008-2016, ciphermail.com.

# Contents

1	Introduction	3
2	S/MIME           2.1         PKI           2.2         X.509 certificate           2.3         Revocation checking	<b>3</b> 3 4 6
3	Gateway S/MIME quick setup3.1Certificate Authority (CA)3.2Certificates for internal users3.3Certificates for external users	<b>6</b> 6 7 9
4	<ul> <li>Email clients setup</li> <li>4.1 Outlook <ul> <li>4.1.1 Importing the pfx attachment</li> <li>4.1.2 Receiving and sending S/MIME</li> <li>4.1.3 Sending signed and encrypted email</li> </ul> </li> <li>4.2 Outlook Express <ul> <li>4.2.1 Importing the pfx attachment</li> <li>4.2.2 Receiving and sending S/MIME</li> <li>4.2.3 Sending signed and encrypted email</li> <li>4.3 Thunderbird</li> <li>4.3.1 Importing the pfx attachment</li> <li>4.3.2 Receiving signed and encrypted email</li> <li>4.3.3 Sending signed and encrypted email</li> <li>4.3.4 Apple Mail</li> <li>4.4 Apple Mail</li> <li>4.5 Gmail</li> <li>4.5 Gmail</li> <li>4.5 Installing the Firefox add-in</li> <li>4.5 Sending signed and encrypted email</li> </ul> </li> </ul>	<b>11</b> 11 14 16 16 17 18 20 21 25 26 27 27 28 28 28 29 29 33
	<ul> <li>4.5.4 Sending signed and encrypted email</li></ul>	33 35 36 36 37 40
A	Ciphermail S/MIME headers	41
в	Links	42

# 1 Introduction

The first part of this guide will give a short introduction on S/MIME. The second part of this guide will briefly explain how to setup a Ciphermail gateway for S/MIME (for a more detailed guide on managing a Ciphermail gateway see the *Ciphermail Administration Guide*). The third part of this guide will explain how to setup S/MIME for some of the most popular email clients (like Outlook, Lotus Notes etc.).

# 2 S/MIME

S/MIME is a widely supported email encryption standard. S/MIME is natively supported by most common email clients like Outlook, Outlook express, Windows Mail, Lotus Notes, Thunderbird, Evolution, Apple Mail, BlackBerry etc. This section will give a brief introduction to S/MIME. S/MIME is based on *Public Key Infrastructure* (PKI) and uses X.509 certificates.

**Note:** this section is a direct copy of the S/MIME section of the *Ciphermail Administration Guide* and can be skipped if the section has already been read.

## 2.1 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 neighbors in a mesh like structure (a web). **For example:** *Alice* trusts *Bob* and *Ted* trusts *Alice* and therefore *Ted* now also trusts *Bob* (through *Allice*). 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.

## 2.2 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*<sup>1</sup> calculated over the bytes of the encoded certificate. The thumbprint uniquely identifies a certificate. The default algorithm used by Ciphermail for calculating the thumbprint is *SHA-512*.

#### 2.3 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 the Certificate Trust List section in the *Ciphermail Administration Guide*.

# 3 Gateway S/MIME quick setup

Ciphermail supports S/MIME encryption and digital signatures. Both the sender and receiver require a certificate and private key. Ciphermail therefore has a built-in CA server that can be used to issue certificates and keys to internal and external users for free.

External users, without a Ciphermail gateway, can use any S/MIME capable email client to start sending en receiving encrypted email once the certificate has been installed. External and internal users however are not required to use the built-in CA. If an external recipient already possesses an S/MIME certificate, the certificate can be used instead.

What now follows is a quick-start-guide on setting up a Ciphermail gateway for S/MIME. It is assumed that the Ciphermail gateway is already setup and is capable of sending email.

# 3.1 Certificate Authority (CA)

The Ciphermail 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.

A brief explanation of the CA functionality will now follow. This section can be skipped if a CA is already setup.

 $<sup>^1</sup>See \ http://en.wikipedia.org/wiki/Cryptographic_hash_function for more info on cryptographic hash functions.$ 

**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).

#### **Creating new CA**

A new CA can be created by clicking *Create new CA* on the CA page ( $CA \rightarrow Create$  new CA). The *Create new CA* page will be opened (see figure 1).

With the following steps, a new CA can be created:

- 1. Set validity to 1825 days (5 years) and key length to 2048<sup>2</sup>.
- 2. Leave the email field empty.
- 3. Set a common name that uniquely identifies your CA. The common name of the root must be different from the common name of the intermediate.
- 4. Select make default CA.
- 5. Set signature algorithm to SHA1 With RSA<sup>3</sup>.
- 6. Click Create to create the new root and intermediate certificate.

# 3.2 Certificates for internal users

For every internal user an S/MIME certificate should be created. The domains for which email is received should be internal domains and should be set to allow encrypted S/MIME messages to be sent.

For every domain for which you receive email do the following:

- 1. Add the domain.
- 2. Set *Encrypt mode* to Allow<sup>4</sup>.
- 3. Set the Locality property to Internal.
- 4. Set the S/MIME Allow property.

For every internal user (i.e., a user from an internal domain) do the following:

- Create a new end-user certificate by clicking CA (this opens the Create end-user certificate page, see figure 2)
- 2. Set validity to 1825 days (5 years) and key length to 2048<sup>5</sup>.

<sup>&</sup>lt;sup>2</sup>2048 is the best compromise between security and key length.

<sup>&</sup>lt;sup>3</sup>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*.

<sup>&</sup>lt;sup>4</sup>Alternatively *No Encryption* can be used in combination with a *Subject trigger*.

<sup>&</sup>lt;sup>5</sup>2048 is the best compromise between security and key length.

Certificates	Roots	CRLs	CA	DLP	Settings	Queues
Create ne	w CA					
The built-in	Certificate	Request H	andler	requires a	root and int	ermediate (
Root certificat	e					
	Validity 1	825				
Key	in bits	.048 🗘				
	Email					
Commo	n name					
more						
Intermediate	certificate					
	Validity in days	825				
Key	in bits	.048 🌲				
	Email					
Commo	n name					
□ more						
General						
Make def	ault CA 😡	r				
Signature al for c s	gorithm ertificate signature	iha1 With Rsa	*			
Create	Cancel					

Figure 1: Create new CA

- 3. Set signature algorithm to SHA1 With RSA<sup>6</sup>.
- 4. Set email to the email address of the internal user.
- 5. Set a common name to identify the user (for example use the first and last name of the user).
- 6. Click Create to create the certificate and private key for the user.

**Note:** For advanced settings like CRL distribution point see the *Ciphermail Administration Guide* for more information.

#### 3.3 Certificates for external users

In order to send and receive S/MIME encrypted and digitally signed email, every external recipient should possess a certificate and private key. An external recipient can request a certificate from an external CA (for example from Verisign). However, getting a certificate from Ciphermail's built-in CA is much simpler than requesting a certificate from an external CA. With Ciphermail's built-in CA, the external user only need to install a password protected pfx file.

**Note:** the email address of the CA should be specified before the password protected pfx file can be sent. For more information, see *CA email* setting in section *CA settings* of the *Ciphermail Administration Guide*.

For each external recipient requiring an S/MIME certificate do the following:

- 1. Create a new user.
- 2. Set the S/MIME Allow property.
- 3. Create a new end-user certificate by clicking CA (this opens the *Create* end-user certificate page, see figure 2)
- 4. Set validity to 1825 days (5 years) and key length to 2048<sup>7</sup>.
- 5. Set signature algorithm to SHA1 With RSA<sup>8</sup>.
- 6. Set email to the email address of the external user.
- Set a common name to identify the user (for example use the first and last name of the user).
- If the certificate and private key should be sent by email to the external recipient in a password encrypted pfx file, select Send by email and select a secure password <sup>9</sup>.

<sup>&</sup>lt;sup>6</sup>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*.

<sup>&</sup>lt;sup>7</sup>2048 is the best compromise between security and key length.

<sup>&</sup>lt;sup>8</sup>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*.

<sup>&</sup>lt;sup>9</sup>the 'gear' icon generates a secure random password

create new end-	user certificate
On this page, a certifi	cate and private key for an end-user can be created. The c
create CRL   send certi	ficates   bulk request   pending requests
General	
validity	1825
Key length in bits	2048 🤤
Signature algorithm for certificate signature	Sha1 With Rsa 💲
Certificate subject	
Email required	
Common name required	persona non-validated
□ more	
Email delivery	
Send by email send key file to user	
Password password for key file	() 🌼
SMS password send password via SMS	
Store password store the pfx password in the user preferences	
Advanced	
Show advanced se	ettings
Add CRL dist. point add to certificate	
CRL dist. point fully qualified URL	
Certificate Authority the CA to use for the certificate request	built-in 🛟
Add user add a user object for the requested certificate	8
Request	

Figure 2: Create end-user certificate

- 9. If the recipient should receive the pfx password via an SMS Text message, select *SMS password*. The recipients telephone number should be set for the external user.
- 10. Click *Create* to create the certificate and private key for the user.

After the certificate has been created, the certificates will be added to the certificate store. If *Send by email* was selected, the certificate and private key will be stored inside a password encrypted pfx file and a message with the pfx file will be sent to the recipient. If the *SMS password* was selected, the password for the pfx file will be sent to the recipient via an SMS Text message. If the password was not sent via an SMS Text message, an alternative channel should be used to let the recipient know what the password is.

The pfx file with the certificate and private key should be installed on the recipients email client. The next sections will briefly explain the pfx file installation procedures for some of the most used email clients.

# 4 Email clients setup

The next sections will explain the pfx file installation procedures for some of the most used email clients.

# 4.1 Outlook

## 4.1.1 Importing the pfx attachment

An Outlook recipient receives a message with the password encrypted pfx file as an attachment (see figure 3).



Figure 3: Outlook pfx attachment

The pfx file can be imported with the following procedure:

- 1. Start the "certificate import wizard".
- 2. Go to password page.
- 3. Enter the private key password.
- 4. Go to finish page.
- 5. Accept the trusted root certificate.

These steps will now be explained in more detail.

**1. Start the "certificate import wizard"** Double click the attached pfx file (alternatively save the pfx file and open it with the file Explorer). A warning will be shown asking whether the pfx file should be opened (see figure 4). Click on the *Open* button. The *certificate import wizard* will now be started.

Opening	Mail Attachment	? ×				
You should only open attachments from a trustworthy s						
	Attachment: key.pfx from Inbox - Microsoft O	utlook				
	Would you like to open the file or save it to you	ur computer?				
	Open Save	Cancel				
	Always ask before opening this type of file					

Figure 4: Outlook open pfx file

**2. Go to password page** Click Next button until the password page (see figure 5).

**3. Enter the private key password** Enter the pfx file password (see figure 6). The following two options can optionally be enabled: *Enable strong private key protection* and *Mark this key as exportable* 

**Enable strong private key protection** If this option is selected Windows will always ask for permission when a program tries to access the private key.

**Mark this key as exportable** If this option is selected, the private key can be exported to create a backup of the private key.

**4. Go to finish page** Click next until the finish page (see figure 7).



Figure 5: Certificate import wizard

Certificate Import Wizard	×
Password	
To maintain security, the private key was protected with a password.	
Type the password for the private key. Password: Enable strong private key protection. You will be prompted every time the	
private key is used by an application if you enable this option.	
Mark this key as exportable. This will allow you to back up or transport your keys at a later time.	
< Back Next > Cancel	

Figure 6: Enter pfx password

**5. Accept the trusted root certificate** On the final page, click *Finish* to start the certificate and private key import procedure. The pfx file not only contains an end-user certificate and private key, but also the root and intermediate certificates. The import wizard will try to import the root and intermediate certificates. When importing a root certificate a warning dialog is shown asking for permission to import the root certificate (see figure 8). Click *Yes* to accept the root certificate.

Certificate Import Wizard			X
You have successfully completed the Certificate Import wizard.			
	You have specified the follow Certificate Store Selected Content File Name	wing settings: Automatically determined by t PFX C:\Documents and Settings\m	
	< Back	Finish Cancel	

Figure 7: Certificate wizard finish

Warning: Only accept the root certificate if it comes from a trusted entity.

Securi	ty Warning
⚠	You are about to install a certificate from a certification authority (CA) claiming to represent: Djigzo root
	Windows cannot validate that the certificate is actually from "Djigzo root". You should confirm its o
	Thumbprint (sha1): C48F8086 6881E5AD 9ECD50FB AD417E04 5A89F168
	Warning: If you install this root certificate, Windows will automatically trust any certificate issued by this CA. acknowledge this risk.
	Do you want to install this certificate? Yes No

Figure 8: Certificate wizard root import warning

#### 4.1.2 Receiving and sending S/MIME

Now a certificate and private key have been installed, S/MIME encrypted and digitally signed email can be sent and received. An example of a signed an encrypted email in Outlook is shown in figure 9.

The "padlock" indicates that the message was encrypted and the "ribbon" indicates that the message was signed (see figure 10) The signed and encrypted message contains the public certificate of the sender. To make it pos-

From: To: Cc:	Martijn Brinkers [martijn@djigzo.com] test@mitm.nl	Sent:	Mon 5/25/2009	1:18 PM
Subject: Signed By:	test encrypted email m.brinkers@pobox.com		l	
This is	a signed and encrypted email.			Î
Regards,				
Martijn	Brinkers			=
 Djigzo d	open source email encryption gateway www	v.dji	gzo.com	•

Figure 9: Outlook signed and encrypted

sible to reply to the message, the public certificate should be associated with the sender. This can be done by clicking the senders email address then right-click and select *Add to Outlook Contacts* (see figure 11).



Figure 10: Outlook sign and encrypt icons

From: To:	Martijn Brin test@mitm.		Martijn Brinkers [martijn@djigzo.com]	Sent:	Mon 5/25/2	009 1:18 PM
Cc			Sch <u>e</u> dule a Meeting			
Subject: Signed By:	test encryp m.brinkers	P	Send <u>M</u> ail Sign In to Instant Messaging			
This is	a signe	ą	Reply All with Instant Message			-
			Additional Actions			
Regards,			Send <u>O</u> ptions			
0.1		2	Add to Outlook Contacts			=
Martijn	Brinker	8	Look up O <u>u</u> tlook Contact			
			Outloo <u>k</u> Properties			
Djigzo o	pen sou		Cop <u>v</u>	w.dji	gzo.com	
						•

Figure 11: Outlook add to contacts

Now save the newly added Outlook contact. If the contact is already part of your contacts you will receive a "Duplicate Contact Detected" (see figure 12).

Duplicate Contact Detected ? × The name or email address of this contact already exists in the Contacts folder. Would you like to: O Add new contact Opdate information of selected Contact. A backup copy will be saved in Deleted Items Folder Full Name Job Title Company E-mail Martijn Brinkers martijn@djigzo.com Preview of Updated Business Card: Changes to Selected Contact: Full Name: Martijn Brinkers **Martijn Brinkers** E-mail: martiin@diigzo.com Contact Picture: No change martijn@djigzo.com Votes: No change Update Cancel

Click Update to add the certificate to the contact.

Figure 12: Outlook duplicate contact

**Note:** You only need to associate the certificate with the sender contact the first time you receive a signed and encrypted email.

#### 4.1.3 Sending signed and encrypted email

Sending a signed and encrypted email with Outlook is similar to sending a normal non-encrypted email. Sign and encrypt is triggered by selecting the sign and encrypt options. Outlook 2007 adds these icons to the toolbar (see figure 13). With older versions of Outlook the sign and encrypt icons can be manually added to the toolbar or the sign and encrypt option can be selected by opening the message options and selecting the *Security Settings...* (see figure 14).

In order to encrypt an email for a recipient, the certificate of the recipient must be available. If Outlook cannot find a certificate for one of the recipients a warning will be shown (see figure 15).

A message cannot be encrypted when the recipient does not have a certificate associated with the contact. A copy of the recipients certificate can be directly imported into the associated contact. To do this, open the contact and select the *Certificates* for the contact<sup>10</sup> (see figure 16) and import the certificate file (.cer or .p7b).

#### 4.2 Outlook Express

An Outlook Express recipient receives a message with the password encrypted pfx file as an attachment (see figure 17).

<sup>&</sup>lt;sup>10</sup>In Outlook 2003 you should open the *Certificates* tab.

signed and encrypted	_ = X
Message Insert Options Format Text	۲
Calibri (Bo * 11 * A* A* Ξ * Ξ * 🖤)         Paste         Ø         B       I         B       I         B       I         B       I         B       I         B       I         I       Inductor         I       Inductor	Follow Up + Contians
Send Subject: signed and encrypted	Encrypt Encrypt this message to make it harder for unauthorized people to read it.
This email should be signed and encrypted Martijn	ā Î



Message Option	5
Message settings	Security
Importa	Security Properties
Sensitiv	C Encrypt message contents and attachments
Voting and Trackir	Add digital signature to this message
🕢 🗖 🗆 Use	Send this message as clear text signed
🖉 🗆 🗆 Rec	Request S/MIME receipt for this message
🗖 Rec	Security Settings
Delivery options -	Security setting:
📺 🗆 Нал	<automatic> Change Settings</automatic>
Ŭ □ Do	Security Label
🗖 Exp	Policy Module: <none> Configure</none>
Attachr	Classification:
Encodir	Privacy Mark:
Contacts	
Categories	OK Cancel

Figure 14: Outlook security properties

# 4.2.1 Importing the pfx attachment

Importing the pfx from Outlook Express is similar to importing from Outlook. See section 4.1.1 for a detailed explanation on how to import the pfx attachment.



Figure 15: Outlook encryption problems

😱 🖬 " Ŭ 🌢 🧇	÷	test - Contact	_ = X				
Contact Inser	t Format Text						
Save & New *	General     Certificates       Details     All Fields       Activities	E-mail Meeting Call	ABC Spelling				
Actions	Show	Communicate	Proofing				
Certificates (Digital IDs):	Certificates (Digital IDs): Properties						
		Set	as Default				
			Import				
			Export				
			Remove				

Figure 16: Outlook contact certificates

#### 4.2.2 Receiving and sending S/MIME

Now a certificate and private key have been installed, S/MIME encrypted and digitally signed email can be sent and received. An example of a signed an encrypted email in Outlook Express is shown in figure 18.

The "padlock" indicates that the message was encrypted and the "ribbon" indicates that the message was signed (see figure 19) Outlook Express automatically associates the certificate of the sender with the senders contact.

#### 4.2.3 Sending signed and encrypted email

Sending a signed and encrypted email with Outlook is similar to sending a normal non-encrypted email. Sign and encrypt is triggered by selecting the sign and encrypt options (see figure 20)

! 🛛 🏹 From	Subject	Received 🛆						
0 📄 ca@djigzo.com	Your email encryption certificate	5/25/2009 3:47 PM						
From: ca@djigzo.com To: test@mitm.nl Subject: Your email encryption certificate		R						
Hi,		🖓 key.pfx (5.49 KB)						
		Save Attachments						
Attached you will find a certificate with a private key which you can use to encrypt and de email.								
The password for the encrypted ke	ey was sent to you by SMS to	number 3161134****.						
The SMS can be identified by 109	7.							
 D''								
Djigzo open source email encryptio	on 							
	U Working Online							

Figure 17: Outlook Express pfx attachment



Figure 18: Outlook Express signed and encrypted



Figure 19: Outlook Express sign and encrypt icons

This message should be signed and encrypted											
File	Edit	View	Insert	Format	Tools	Messa	ige Help	I			<b>.</b>
		X			<b>9</b>	9.	ABC			5	
Send		Cut	Сору	Paste I	Undo	Check	Spelling	Sign	Encry	Offline	
🛐 To:	m	artijn@c	ljigzo.com	ı					Encryp	<mark>t message</mark>	<b>R</b>
🛐 Cc:	Γ										6
Subject:	Th	nis mess	age shoul	ld be signe	d and en	crypted					
Arial	_		•	10 💌	Ē,   ₽	3 I (	UA,	ŧŧ		- 🐁 🖬	2
								<b></b>			
A signed and encrypted message									-		
, 											

Figure 20: Outlook Express sign and encryption options

## 4.3 Thunderbird

A Thunderbird recipient receives a message with the password encrypted pfx file as an attachment (see figure 21).



Figure 21: Thunderbird pfx attachment

#### 4.3.1 Importing the pfx attachment

The pfx file can be imported with the following procedure:

- 1. Save the pfx file to the desktop.
- 2. Open the certificate manager.
- 3. Import the pfx.
- 4. Set the master password.
- 5. Enter the pfx password.
- 6. Lookup the name of the imported root.
- 7. Enable the imported root for S/MIME.
- 8. Select a signing and encryption certificate.

These steps will now be explained in more detail.

**1. Save the pfx file to the desktop** The pfx attached to the messages should be saved before the pfx can be imported. The the key.pfx attachment should be saved to the desktop (or to any other location normally used for attachments).

**2. Open the certificate manager** Open the Thunderbird options dialog (Tools $\rightarrow$ Options<sup>11</sup>). Select the *Advanced settings* and select the *Certificates* tab (see figure 22). Now click *View Certificates*. The *Certificate Manager* will now be opened (see figure 23).



Figure 22: Thunderbird certificates options

**3. Import the pfx** On the *Certificate Manager* select the *Your Certificates* tab, click the *Import* button and select the pfx file which was previously saved in step 1.

 $<sup>^{11}\</sup>text{On}$  some Thunderbird versions the options dialog should be opened with  $\textbf{Edit} {\rightarrow} \textbf{Preferences}$ 

our Certificates	Other People's	Web Sites	Authorities		
You have certifica	ates from these or	ganisations	that identify yo	iu:	
Certificate	Security D	Pur	Serial Nu	Expir	<b></b>
		D. J	1 Turnet		
New	раскир	Dackup All	Import	Dele	ue -

Figure 23: Thunderbird certificate manager

**4. Set the master password** The first time a certificate is added to Thunderbird, the *Master Password* for the key store should be set (see figure 24). The master password is used to protect the private keys which are stored in Thunderbird. The private keys are encrypted with the *Master Password* to ensure that only the owner can access the private keys.

**Note:** this is NOT the password of the pfx file from step 1! A secure master password should be selected by the computer owner or administrator. If the master password was already set, the master password should be entered before a new certificate can be imported.

Change Master Password	×
Security Device: Software Security Device	
Current password: (not set)	
New password:	
New password (again):	
Password quality meter	
OK Cancel	

Figure 24: Thunderbird master password

**5.** Enter the pfx password The password for the pfx file should now be entered (see figure 25). This is the password that was provided via an SMS Text message or provided by other means. Clicking *OK* will start the import process.

Password Entry Dialogue		×
Please enter the password certificate backup.	I that was used to encrypt this	
Password:		
	OK Cance	

Figure 25: Thunderbird password entry dialog

**6.** Lookup the name of the imported root The imported root certificate is not yet enabled for S/MIME. Before the root certificate can be enabled for S/MIME the name of the root certificate should be looked up first. Open the *Certificate Manager*, select the *Your Certificates* tab and select the certificate that was just imported (see figure 26).

Double click the certificate to open the certificate details page (see figure 27). The first entry in the *Certificate Hierarchy* is the root certificate. The name of the root certificate is needed in the following steps.

🍣 Certificate M	anage	er			_ 🗆 ×
Your Certificates	Othe	r People's 🛛 Web Sites	Authorities		
You have certific	ates fr	om these organisation	is that identify y	/ou:	
Certificate Nan	ne	Security Device	Purposes	Serial Number	Expires O 🖽
🖃 Djigzo email e	ncr				
<sup>i</sup> persona n	on	Software Security	<unknown></unknown>	01:21:76:F6:9E:	5/24/2014
⊻iew	Bad	:kup Backup All	Import	Delete	
					ОК

Figure 26: Thunderbird manager your certificates

**7. Enable the imported root for S/MIME** Open the *Certificate Manager* and select the *Authorities* tab (see figure 28). Select the root certificate from step 6 and click the *Edit* button to open the *Edit CA certificate trust settings* page.

On the *Edit CA certificate trust settings* page, select "This certificate can identify mail users" to enable the root certificate for S/MIME (see figure 29). Click *OK* and close all dialogs.

8. Select a signing and encryption certificate Now that a certificate and private key have been imported, the encryption and signing certificate should

Certificate Viewer:"82450CCEDE7C38590825438B362C3FEEF912C76AF9D3 🗙
General Details
Certificate Hierarchy
🗖 Djigzo root
😑 Djizgo intermediate
-persona non-validated
Certificate Fields
🖃 Djigzo root - Djigzo email encryption 📃
- Certificate
Version
Serial Number
🔁 Validity
-Not After
Field Value



🥞 Certificate Manager	
Your Certificates Other People's Web Sites Authorities You have certificates on file that identify these certificate authorities:	
Certificate Name Security Device	
Digge intermediate     Digge root     Digge root     Software Security Device     Digge root     Software Security Device	
View Edit Import Delete	
	ОК

Figure 28: Thunderbird authorities

Edit CA certificate trust settings	×
The certificate "Djigzo root" represents a Certificate Authority.	
Edit trust settings:	
This certificate can identify web sites.	
This certificate can identify mail users.	
🗖 🌃 certificate can identify software makers.	
OK Cancel	

Figure 29: Thunderbird CA certificate trust settings

be selected. Open the *Account Settings* page (*Tools* $\rightarrow$ *Account Settings...*<sup>12</sup>). Now select the security options of the email account for which the signing and encryption certificate should be set (see figure 30).

To select a signing and encryption certificate, click the *Select...* button for *Digital Signing* and *Encryption* and select the newly added certificate. Leave all other settings to their default values and close the account settings dialog.

Thunderbird is now ready for sending and receiving signed and encrypted email.

counc sectings	
mail.mitm.nl	Security
-Copies & Folders -Composition & Addressing -Disc Space -Junk Settings -Return Receipts -Security -Local Folders -Disc Space	To send and receive signed or encrypted messages, you should specify both a digital signing certificate and an encryption certificate. Digital Signing Use this certificate to digitally sign messages you send: Select Clear Digitally sign messages (by default) Encryption
<sup>i</sup> …Junk Settings Outgoing Server (SMTP)	Use this certificate to encrypt & decrypt messages sent to you:           Select         Clear           Default encryption setting when sending messages: <ul> <li>Never (do not use encryption)</li> </ul>
<u>A</u> dd Account Set as De <u>f</u> ault	C Required (can't send message unless all recipients have certificates) Certificates
<u>R</u> emove Account	View Certificates Security Devices

Figure 30: Thunderbird Account Settings

#### 4.3.2 Receiving signed and encrypted email

An example of a signed an encrypted email in Thunderbird is shown in figure 32. The "padlock" indicates that the message was encrypted and the "ribbon" indicates that the message was signed (see figure 31)

	>
--	---

Figure 31: Thunderbird sign and encrypt icons

 $<sup>^{12}\</sup>mbox{On}$  some Thunderbird versions the Account Settings should be opened with  $\textbf{Edit} {\rightarrow} \textbf{Account}$  Settings...

ኑ	$\star$ 0		Subject	63	Sender	۵	Date		₽.
	• 0	]	Your email encryption certif		ca@djigzo.com		3:39 PM		
	٠		test signed and encrypted	•	Martijn Brinkers	•	4:00 PM		
	Subj	ect:	test signed and encrypted						-
	Fr	om:	<u>Martijn Brinkers <martijn@djig< u=""></martijn@djig<></u>	20.00	om>				
	Da	ate:	4:00 PM					ſ	7
		To:	<u>test@mitm.nl</u>						
Tł	his m	ess	sage is signed and e	ncr	vpted				
					<b>JF</b>				
	-								
D	jigzo	0]	pen source email enc	ryp	)tion gateway <u>t</u>	ww.	djigzo	.con	2
1					Ur	nread	: 0 Tot	al: 2	//

Figure 32: Thunderbird signed and encrypted

### 4.3.3 Sending signed and encrypted email

A message in Thunderbird can be signed and encrypted by selecting *Encrypt This Message* and *Digitally Sign This Message* from the *Security* pull-down menu (see figure 33).



Figure 33: Thunderbird sign and encrypt

#### 4.4 Apple Mail

#### 4.4.1 Importing the pfx attachment

The pfx file can be imported with the following procedure:

- 1. Start the Keychain Access application.
- 2. Enter the pfx password.
- 3. Accept the root certificate.
- 4. Restart Mail.

These steps will now be explained in more detail.

**1. Start the Keychain Access application** By double-clicking the pfx file, the *Keychain Access* application will be started. The *Keychain Access* application will automatically start the certificate and private key import process. If the *Keychain Access* application is not automatically opened, drag the pfx file onto the *Keychain Access* application icon<sup>13</sup>.

**2. Enter the pfx password** The password for the pfx file should now be entered. This is the password that was provided via an SMS Text message or provided by other means.

**3.** Accept the root certificate The pfx file not only contains the end-user certificate and private key but also the root and intermediate certificate. When import a root certificate, the *Keychain Access* application asks whether the root certificate should be trusted<sup>14</sup> (see figure 34). Select *Always trust*.

R	Wilt u dat uw computer vanaf nu certificaten vertrouwt die door 'Djigzo root' zijn ondertekend? Dit certificaat wordt als vertrouwd gemarkeerd voor alle gebruikers van deze computer. Om dit besluit later te wijzigen, opent u het certificaat in Sleutelhangertoegang en past u de vertrouwensinstellingen aan.
🔯 Djigzo re	pot
Certificate	Djigzo root Rootcertificaatautoriteit Verloopt op: dinsdag 13 mei 2014 20:36:44 GMT+02:00 S Dit rootcertificaat wordt niet vertrouwd
▶ Vertrouw ▶ Details	
	(Verberg certificaat) (Vertrouw niet) (Vertrouw altijd)

Figure 34: Apple Mail trust root certificate

<sup>&</sup>lt;sup>13</sup>/Applications/Utilities

<sup>&</sup>lt;sup>14</sup>This example is in Dutch. Dialogs for other languages should look similar.

**4. Restart Apple Mail** After installing the private key, Apple Mail should be restarted. Apple Mail is now setup for sending and receiving signed and encrypted email.

#### 4.4.2 Receiving signed and encrypted email

An example of a signed an encrypted email in Apple Mail is shown in figure 35.

00	Usir	ng encryp	tion and	digital	signatures in Mail	$\subset$	)
$\otimes$				4			
Delete	Reply	Reply All	Forward	Print			
From: Subject: Date: To: Security:	Martijn Antw.: 23 me Daan Daan	n Brinkers < : test mailt i 2009 19: Hansen rypted, 🗱 S	cmartijn@@ <b>jes</b> 30:09 GMT Signed	djigzo.co [+02:00	om>		
_							

Figure 35: Apple Mail signed and encrypted

#### 4.4.3 Sending signed and encrypted email

A message can be signed and encrypted by selecting the sign and encrypt options in the compose window (see figure <u>36</u>).

4	*

Figure 36: Apple Mail sign and encrypt buttons

# 4.5 Gmail

If Gmail is accessed via the Gmail web interface, a dedicated browser addin is required for reading and sending S/MIME messages since Gmail does not natively support S/MIME. A cross-platform add-in is available for Firefox with which S/MIME encrypted email can be sent and received directly from the Gmail web interface.

**Note:** If Gmail is accessed with POP3 or IMAP using an email client, like for instance Outlook, see the guide for the specific email client. This section only explains how to use S/MIME with the Gmail web interface.

#### 4.5.1 Installing the Firefox add-in

The Gmail add-in can be downloaded from https://addons.mozilla.org/ en-US/firefox/addon/592. The add-in can be installed by clicking *Add to Firefox*.

#### 4.5.2 Importing the pfx attachment

A Gmail recipient receives a message with the password encrypted pfx file as an attachment (see figure 37).

```
      <u>Archive</u>
      Report spam
      Delete
      Move to ▼
      Labels ▼
      More actions ▼

      Your email encryption certificate
      Inbox
      X
```

$\stackrel{\text{tr}}{=}$	ca@djigzo.com to me	show details 1:33 PM (8 minutes ago) 🖉 🦘 Reply   🔻
Hi	1	
At yo	tached you will find a certificate with our email.	a private key which you can use to encrypt and decrypt
Tł	e encrypted key requires a password	l which should have been handed out to you.
 Dj	igzo open source email encryption	
[	⊇ <mark>key.pfx</mark> 9K <u>Download</u>	
◆ [	Reply 🔿 Forward	

Figure 37: Gmail pfx attachment

The pfx file can be imported with the following procedure:

- 1. Save the pfx file to the desktop.
- 2. Open the certificate manager.
- 3. Import the pfx.
- 4. Set the master password.
- 5. Enter the pfx password.
- 6. Lookup the name of the imported root.
- 7. Enable the imported root for S/MIME.

These steps will now be explained in more detail.

**1. Save the pfx file to the desktop** Because the Gmail add-in works with Firefox, the pfx file must be saved to the desktop (or to any other location) before it can be imported into Firefox.

**2. Open the certificate manager** Open the Firefox options dialog from the Firefox menu (Tools $\rightarrow$ **Options**<sup>15</sup>). Select the *Advanced settings* and select the *Certificates* tab (see figure 38). Now click *View Certificates*. The *Certificate Manager* will now be opened (see figure 39).

		5		ST.	0	ič:	
Main	Tabs	Content	Applications	Privacy	Security	Advanced	
ieneral	Network	Update E	ncryption				
- Protoc	ole						
	ie 55L <u>3</u> .0j		, N	Use ILS	<u>I</u> .0		
– Certific	ates —						-
When	a server re	quests my p	ersonal certifica	ate:			
	electione au	itomatically	Ask me e	very time			
C Se	viece one de						
C Se	vioce oulo de						
C Se	Certificates	Revoc	ation Lists	<u>V</u> alidation	Security	Devices	

Figure 38: Firefox certificates options

				1	1.000
Certificate Nam	e	Security Device	Serial Number	Exp	

Figure 39: Firefox certificate manager

**3. Import the pfx** On the *Certificate Manager* select the *Your Certificates* tab, click the *Import* button and select the pfx file which was previously saved in step 1.

<sup>&</sup>lt;sup>15</sup>On some Firefox versions the options dialog should be opened with Edit -> Preferences

**4. Set the master password** The first time a certificate is added to Firefox the *Master Password* for the key store should be set (see figure 40). The master password is used to protect the private keys which are stored in Firefox. The private keys are encrypted with the *Master Password* to ensure that only the owner can access the private keys.

**Note:** this is NOT the password of the pfx file from step 1! A secure master password should be selected by the computer owner or administrator. If the master password was already set, the master password should be entered before a new certificate can be imported.

Change Master Passwor	d	×
Security Device: Softwa	are Security Device	
		h
Current password:	(not set)	
New password:		
New password (again):		
Password quality meter		ן
L <u>'</u>		1
	OK Cancel	

Figure 40: Firefox master password

**5. Enter the pfx password** The password for the pfx file should now be entered (see figure 41. This is the password that was provided via an SMS Text message or provided by other means. Clicking *OK* will start the import process.

Password Entry Dialogue	×
Please enter the password that was used to encrypt th certificate backup.	is
Password:	
OK Ca	ncel

Figure 41: Firefox password entry dialog

6. Lookup the name of the imported root The imported root certificate is not yet enabled for S/MIME. Before the root certificate can be enabled for

S/MIME the name of the root certificate should be looked up first. Open the *Certificate Manager*, select the *Your Certificates* tab and select the certificate that was just imported (see figure 42).

Double click the certificate to open the certificate details page (see figure 43). The first entry in the *Certificate Hierarchy* is the root certificate. The name of the root certificate is needed in the following steps.

🕲 Certificate Mar	nage	r			_ 🗆 ×
Your Certificates	Other	r People's   Web Sites	Authorities		
You have certificat	tes fr	om these organisation	is that identify y	/ou:	
Certificate Name		Security Device	Purposes	Serial Number	Expires O 🖽
🖃 Djigzo email end	:r				
<sup>i</sup> persona nor	ì	Software Security	<unknown></unknown>	01:21:76:F6:9E:	5/24/2014
<u>V</u> iew	Bac	kup Backup All	Import	Delete	
					ОК

Figure 42: Firefox manager your certificates



Figure 43: Firefox certificate details

**7. Enable the imported root for S/MIME** Open the *Certificate Manager* and select the *Authorities* tab (see figure 44). Select the root certificate from step 6 and click the *Edit* button to open the *Edit CA certificate trust settings* page.

On the *Edit CA certificate trust settings* page, select "This certificate can identify mail users" to enable the root certificate for S/MIME (see figure 45). Click OK and close all dialogs.

Gmail is now ready for sending and receiving signed and encrypted email.

🕲 Certificate Manager	_ 🗆 ×
Your Certificates Other People's Web Sites Authorities	
You have certificates on file that identify these certificate authorities:	
Certificate Name Security Device	E.
Djigzo email encryption	
Djizgo intermediate Software Security Device	
<sup>i</sup> Djigzo root Software Security Device	
Entrust, Inc.	•
View Edit Import Delete	
	ОК

Figure 44: Firefox authorities

Edit CA certificate trust settings
The certificate "Djigzo root" represents a Certificate Authority.
Edit trust settings:
This certificate can identify web sites.
This certificate can identify mail users.
Mis certificate can identify software makers.
OK Cancel

Figure 45: Firefox CA certificate trust settings

#### 4.5.3 Sending signed and encrypted email

An example of a signed an encrypted email in Gmail is shown in figure 46.

Note: The Gmail S/MIME add-in currently does not verify digital signatures.

### 4.5.4 Sending signed and encrypted email

A message can be signed and encrypted by selecting the sign and encrypt option (see figure 47).

Click Send to sign, encrypt and send the message. When a message is signed

<u>« Ba</u>	Ck to Inbox         Archive         Report spam         Delete         Move to ▼         Labels ▼         More actions ▼
sigr	ned and encrypted email Inbox   X
1	Martijn Brinkers to me show details 1:55 PM (56 minutes ago) 🖉 🦘 Reply 🔻
Th	is message is signed and encrypted
Dj	igzo open source email encryption gateway www.djigzo.com
	smime.p7m 7K <u>Download</u> Unverified Message: This version of Gmail S/MIME does not support digital signature verification. Signer: E=info@djigzo.com E=m.brinkers@pobox.com CN=Thawte Freemail Member
	Issuer: CN=Thawte Personal Freemail Issuing CA O=Thawte Consulting (Pty) Ltd. C=ZA
€	Reply - Forward

Figure 46: Gmail signed and encrypted

★ Reply     ★ Forward
Send Save Now Discard
To: Martijn Brinkers <martijn@djigzo.com></martijn@djigzo.com>
Add Cc   Add Bcc   Edit Subject 🖉 Attach a file   Include original attachments
B I U F-rT-T₂ T₂ S S S S II I
On Tue, May 26, 2009 at 1:55 PM, <u>Martijn Brinkers</u> <martijn@djigzo.com> wrote: This message is signed and encrypted  Djigzo open source email encryption gateway www.djigzo.com</martijn@djigzo.com>
Send Save Now Discard

Figure 47: Gmail sign and encrypt options

a confirmation dialog will pop-up asking to confirm the signing of the message (see figure 48).

To confirm the signing the master password from step 4 must be entered.

After clicking OK a pop-up dialog will be shown on which the Gmail password

Text Signing Request 🛛 🔀
The site 'mail.google.com' has requested that you sign the following text message:
Content-Type: text/html
Hi this is signed and encrypted
Signing Certificate
82450CCEDE7C38590825438B362C3FEEF912C76AA4B49 💌
Issued to: E=test@mitm.nl,CN=persona non-validated Serial Number: 01:21:76:F6:9E:90:0C:7E:AF:C0:0B:39:43 Valid from 5/24/2009 10:50:22 AM to 5/24/2014 10:50:22 Purposes: Sign,Encrypt Certificate Key Usage: Signing,Key Encipherment Email: test@mitm.nl
To confirm you agree to sign this text message using your selected certificate, please confirm by entering the master password:
OK Cancel

Figure 48: Gmail sign confirmation

should be entered (see figure 49). The Gmail add-in sends the signed and encrypted message via the Gmail SMTP servers. The Gmail password is required for sending the message via the Gmail SMTP servers.

Authent	ication Required	×
?	Enter password for m.brinkers@gmail.com at smtps://smtp.gmail.com	
	Use Password Manager to remember this password.	
	OK Cancel	

Figure 49: Gmail SMTP password

## 4.5.5 Notes

The Gmail S/MIME add-in has some shortcomings compared to S/MIME support in other mail clients.

• Signatures are not verified.

· Drafts are not stored securely.

For more information see <a href="http://richard.jones.name/google-hacks/gmail-smime/gmail-smime.html">http://richard.jones.name/google-hacks/gmail-smime/google

# 4.6 Lotus Notes

A Lotus Notes recipient receives a message with the password encrypted pfx file as an attachment (see figure 50).

🚹 🚰 Home 🚺 🔁 Martijn Brinkers - Inbox 🗙 🚡 > Your email encryption cer	tifica 🗙
Y New 🔻 🥃 Reply 🕶 🍕 Reply To All 👻 🗟 Forward 👻 🚞	) • 🕨 • 前 Display • 🔍 • 🗧
Your email encryption certificate ca to: test	05/26/2009 04:32 PM <u>Show Details</u>
Hi,	
Attached you will find a certificate with s can use to encrypt and decrypt your email.	a private key which you
The encrypted key requires a password which handed out to you.	n should have been
Djigzo open source email encryption	
	🔺 Online 🔺 🥅 🔺

Figure 50: Lotus Notes pfx attachment

#### 4.6.1 Importing the pfx attachment

The pfx file can be imported with the following procedure:

- 1. Save the pfx file to the desktop.
- 2. Open the User Security settings.
- 3. Import Internet Certificates.
- 4. Enter the pfx password.
- 5. Accept all certificates.

These steps will now be explained in more detail.

**1. Save the pfx file to the desktop** The pfx attached to the messages should be saved before the pfx can be imported. The the key.pfx attachment should be saved to the desktop (or to any other location normally used for attachments).

**2. Open the** *User Security* settings Open the *User Security* settings page from main menu File→Security→User Security... (see figure 51).

User Security					
	Certificates	in your ID file			
🕞 Security Basics	Your certifical	tes provide a secure	way to identify you	i to Notes and other program	
🧟 🗆 Your Identity	certificates us	certificates used to secure Notes communications as well as certificates used w			
Your Names			-		
Your Certificates	Your Notes Ce	rtificates	May be used to secure mail with	login to Notes, to access N other Notes users.	
Your Smartcard					
👧 🗉 Identity of Others	Type Issued	i To 🌣	Issu	ed By 🗘	
😤 🗉 What Others Do	🛐 Martijn Brinkers/Martijn Brinkers /Martijn Brinkers			rtijn Brinkers stijn Brinkers	
💝 🗉 Notes Data	ER Martijn Brinkers/Martijn Brinkers /Martijn Brinkers				
🖄 Mail					
	L Colomba d Norra				
	Issued to	Martijn Brinkers/M	artijn Brinkers		
	Issued by	/Martijn Brinkers			
	Activated	05/25/2009	Туре	Notes international encry	
	Expires	05/26/2011	Key identifier	1N6PQ V7J77 W2GUM	
	Advanc	ed Details			

Figure 51: Lotus Notes Your Certificates

**3.** Import Internet Certificates On the User Security page, select Your Identity  $\rightarrow$  Your Certificates and click Get Certificates and select Import Internet Certificates from the pull-down menu (see figure 52). Select the pfx file which was saved in step 1. A pop-up dialog opens in which the file format of the file to import should be selected (see figure 53). Select *PKCS 12 encoded* and click Continue.

**4. Enter the pfx password** The password for the pfx file should now be entered (see figure 54. This is the password that was provided via an SMS Text message or provided by other means. Clicking *OK* will start the import process.

**5.** Accept all certificates The import wizard will now be opened listing all certificates which will be imported (see figure 55). Click *Accept All* to start importing all the certificates.

#### 4.6.2 Receiving signed and encrypted email

The first time a signed and encrypted message is received by Lotus Notes, the signer certificates should be *Cross certified*. Click *Cross certify* to approve the

					? ×		
	Certifi	cates in your ID file					
	Your certificates provide a secure way to identify you to Notes and other programs. Your ID may contain certificates used to secure Notes communications as well as certificates used with the Internet.						
1	Your N	otes Certificates May be u: secure ma	sed to login to N ail with other No	lotes, to access Notes databa tes users.	ases, and to exchange		
	Туре	Issued To 🗘	Issued By 🌣		Get Certificates 🔻		
	R	Martijn Brinkers/Martijn Brinkers	/Martijn Bri	Import (Merge) Notes Certif	icates		
	R	Martijn Brinkers/Martijn Brinkers	/Martijn Bri	Request New Notes Flat Cer	rtificate		
				Import Internet Certificates			
				Request New Interna Certi	ficate		
				Import Internet Certificate f	from a Smartcard		
	Selected item						
	Issue	ed to 🦳 Martijn Brinkers/Martijn Brinkers					

Figure 52: Lotus Notes Import Internet Certificates

S	elect Import File Format 🛛 🔋 🗙
	In what format is your certificate stored in the file?
	○ Binary encoded X.509
	○ Base 64 encoded X.509
	PKCS 12 encoded
	O PKCS 7 encoded
	Continue Cancel

Figure 53: Lotus Notes Import File Format

Enter Password	?	×
Enter the password for the file conta	aining internet certificates.	
Password		
	OK Cancel	]

Figure 54: Lotus Notes PFX password

certificate (see figure 56).

Import Int	tern	et Certificate	:5				?	×
Do you want to accept the following certificates into your ID?								
All Internet	Certi	ficates						
Type Iss	sued	То≎			Issued	ГВу≎		
💽 tes	st@m	nitm.nl			GN=M	artijn		
🚺 💽 tes	st@m	nitm.nl			GN=M	artijn		
🚺 💽 GN	N=Ma	artijn			GN=M	artijn		
🚺 💽 GN	N=Ma	artijn			GN=M	artijn		
Selected ite	em:							
Issued to	0	test@mitm.nl				(Email)	test@mitm.nl	
Issued b	y.	GN=Martijn				(Email)		
Activate	d	05/24/2009	Туре	Internet	multi-pu	urpose		
Expires		05/24/2014	Fingerprint	E111 A	953 AD.	A8 306D C2	20C F94D 407C BF7	7
Advanced Details There is a private key corresponding to this certificate.								
Accept All Cancel								

Figure 55: Lotus Notes confirm import

**Note:** A certificate only need to be cross certified once.

Issue Cross Certificate	? 🗙
Certifier Server	Martijn Brinkers/Martijn Brinkers Local
Subject name	EMAIL=info@djigzo.com/EMAIL=martijn@djigzo.com 💌
Subject alternate names	
Fingerprint	F2C8 1799 7866 F20E 5EE6 1C0D F9A5 78F7
Expiration date	05/26/2019 04:59:28 PM
	Cross certify Cancel

Figure 56: Lotus Notes Cross Certify

A signed and encrypted email can be recognized by clicking the *Security* icon (see figure 57). This opens a pop-up page showing the security details of the

# message.

🚹 🔂 Home	ome 🚺 🦲 Martijn Brinkers - Inbox 🗙 🔀 signed a	and encrypted 🗙
🕙 New 🔻 🚑	Reply 🔻 🐗 Reply To All 👻 📑 Forward 🔻	🕶 🖻 🕶 ኮ 🕶 前 Display 🕶 🔍 🕶 More
	signed and encrypted Martijn Brinkers to: test	05/26/2009 04:59 PM Show Details
History:	This message has been replied to.	
This mess  Djigzo op	age is signed and encrypted. en source email encryption gat	eway www.djigzo.com
	•	Encrypted and Signed by Thawte Freemail Mr

Figure 57: Lotus Notes signed and encrypted

# 4.6.3 Sending signed and encrypted email

A message can be signed and encrypted by selecting the *Sign* and *Encrypt* options on the *Delivery Options* page (see figure 58). The message will be signed and encrypted when the message will be sent.

Delivery Options			? ×
Basic Advanc	ced		OK
Delivery Options			Cancel
Importance:	Normal	🔽 🗖 Return receipt	
Delivery report:	Only on failure	Prevent copying	
Delivery priority:	Normal	Auto spellcheck	
		🧖 Mark Subject Confidential	
<ul> <li>Do not notify i</li> <li>Do not expan</li> </ul>	me if recipient(s) are running Ou d personal groups	it of Office	
Security Options		Mood Stamp	
☑ Sign ☑ Encrypt ☑ Save Gese se	ecurity options as the default	Normal	

Figure 58: Lotus Notes delivery options

# A Ciphermail S/MIME headers

When an incoming email is handled by Ciphermail, special headers about the security properties of the email are automatically added to the email. For example, if an encrypted message sent to an internal users is decrypted by Ciphermail relevant information about the encryption algorithm and recipients is added to the header. Because the message is decrypted by Ciphermail the message is no longer encrypted. The internal recipient can therefore not see that the message was encrypted. Ciphermail therefore adds some security related headers that can be used to check if the message was encrypted and or signed.

The following headers will be added:

```
X-Djigzo-Info-Signer-ID -*
X-Djigzo-Info-Signer-Verified-*
X-Djigzo-Info-Signer-Trusted -*
X-Djigzo-Info-Signer-Trusted-Info-*
X-Djigzo-Info-Encryption-Algorithm -*
X-Djigzo-Info-Encryption-Recipient -*
```

**Note:** The \* is replaced with an index and level as explained below.

[INDEX-]LEVEL

where INDEX and LEVEL are integer numbers starting at 0. INDEX is not used for all headers (optional).

#### Example:

X-Djigzo-Info-Signer-ID-0-0

LEVEL denotes the S/MIME level the values applies to. An S/MIME message supports multiple nested levels of protection (CMS layers). For example, a message can first be signed and then encrypted. LEVEL 0 is the first level found by the S/MIME handler. Multiple items can exist within one level. For example, a message can be encrypted for multiple recipients. INDEX is the index of an item within a level.

#### **Example Headers:**

X-Djigzo-Info-Encryption-Algorithm-0: AES128, Key size: 128

```
X-Djigzo-Info-Encryption-Recipient-0-0:
CN=Thawte Personal Freemail Issuing CA, O=Thawte Consulting (Pty) Ltd.,
C=ZA/6B55D312FF5F9D5DAD9866FF827FFEB5//1.2.840.113549.1.1.1
```

```
X-Djigzo-Info-Encryption-Recipient-1-0:
EMAILADDRESS=support@cacert.org, CN=CA Cert Signing Authority,
OU=http://www.cacert.org, O=Root CA/6683C//1.2.840.113549.1.1.1
```

X-Djigzo-Info-Signer-ID-0-1: CN=UTN-USERFirst-Client Authentication and Email, OU=http://www.usertrust.com, O=The USERTRUST Network, L=Salt Lake City, ST=UT, C=US/88F9874A02A53042E0228D78CBD55795/

X-Djigzo-Info-Signer-Verified-0-1: True

X-Djigzo-Info-Signer-Trusted-0-1: True

The example headers shows that the message was first signed and then encrypted. The encryption algorithm was AES128. The message was encrypted with two certificates:

X-Djigzo-Info-Encryption-Recipient-0-0 X-Djigzo-Info-Encryption-Recipient-1-0

One certificate was issued by Thawte and the other was issued by CACert. The message was signed by one signer with a certificate issued by Usertrust.

**X-Djigzo-Info-Signer-Verified** This headers shows whether the message content was signed and whether the message has not been changed after signing (tampered).

**X-Djigzo-Info-Signer-Trusted** This headers shows whether the signing certificate was trusted (signed by root etc.) by the gateway. If the signing certificate was not trusted, the reason for not trusting the certificate is given in the X-Djigzo-Info-Signer-Trusted header.

**Note:** When email is received by Ciphermail and delivered to an internal user, it will remove all X-Djigzo-\* headers to make sure that an external sender cannot fake any Ciphermail specific headers.

# **B** Links

# Outlook

Using S/MIME in Microsoft Outlook http://searchexchange.techtarget. com/generic/0,,sid43\_gci1252311,00.html

Installing and using your certificate in Microsoft Outlook 2003 http:// www.globalsign.com/support/personal-certificate/per\_outlook03.html

**Overview of certificates and cryptographic e-mail messaging in Outlook** http://office.microsoft.com/en-us/outlook/HP012305341033.aspx?pid= CH100622191033 Configuring S/MIME Security with Outlook Web Access 2003 http:// www.msexchange.org/tutorials/Configuring-SMIME-Security-Outlook-Web-Access-2003. html

Implementing Outlook Web Access with the S/MIME Control http://technet.microsoft.com/en-us/library/aa998939(EXCHG.65).aspx

# Apple

How to Use a Secure Email Signing Certificate (Digital ID) http://support. apple.com/kb/TA22353?viewlocale=en\_US

S/MIME for Apple Mail http://joar.com/certificates/

# Webmail

**Gmail** http://richard.jones.name/google-hacks/gmail-smime/gmail-smime. html