

PrivateFile Application Suite

What is PrivateFile Application Suite?

It is an easy to use set of encryption applications to help you and your company, encrypt sensitive documents and email attachments using the latest (AES) encryption standard. Each application uses the *PrivateFile* encryption engine.

The suite encompasses the following:

- *PrivateFile Desktop*
- *PrivateFile Mail Gateway*
- *PrivateFile Server*

Because all elements use the *PrivateFile* engine, they are fully interoperable. For example, a document encrypted by *PrivateFile Mail Gateway*, can be decrypted by the *PrivateFile Desktop* etc.

PrivateFile Desktop

PrivateFile Desktop integrates directly into the Windows environment. It can run as a stand-alone application or integrates directly into Windows Explorer. The *PrivateFile KeyStore* provides a convenient place to keep regularly used keys. You can *encrypt and send* documents directly from Microsoft Word or Excel.



PrivateFile Mail Gateway

The *PrivateFile Mail Gateway* integrates into the corporate email infrastructure. It automatically encrypts email attachments based on a user-defined set of rules. For example, a rule can be setup which automatically encrypts any email attachments going from *companya.com* to *companyb.com*. In addition the *Mail Gateway* can send emails encrypted using *PGP* version 8 - where *PGP* is installed.

PrivateFile Server

PrivateFile Server is a component that integrates into your corporate applications, allowing them to encrypt and decrypt files using the *PrivateFile* encryption engine.

AES – Advanced Encryption Standard

The Advanced Encryption Standard (AES) is the successor to the Data Encryption Standard (DES). This is an encryption algorithm that has been approved by the US Federal Information Processing Standard (FIPS) for use by U.S. Government organisations. The *PrivateFile* encryption engine uses this as the underlying mechanism for encryption.



PrivateFile Limited

Information Security Centre
2052 Citywest Business Campus
Co. Dublin
Ireland

T +353 (0)1 642 0550
F +353 (0)1 466 0468
E info@private-file.com
W www.private-file.com

PrivateFile Desktop



What is PrivateFile Desktop?

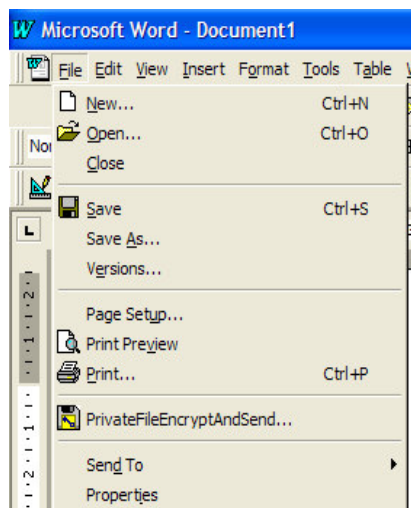
Anyone who has access to your PC or shared folders can also have full access to your potentially critical documents. *PrivateFile* helps you secure your documents and email attachments. It uses the latest AES encryption technology to protect your sensitive information from prying eyes.

PrivateFile runs either as a stand-alone application, integrates directly into your Windows Explorer or into applications such as Microsoft Word or Excel. Simply right-click on a file and choose *encrypt* and enter your encryption key. Your encrypted file is now safe.

PrivateFile includes lots of other features to assist you protect your documents and email attachments.

Main Features:

- Easy Encryption/Decryption of Files, Documents and email attachments.
- Self-Decrypting Executable so that recipient does not need to have PrivateFile installed to decrypt a document sent via email.
- Integrated into Windows Explorer or stand-alone application.
- Integration into Word and Excel to enable *Encrypt and Send* functionality. You can easily encrypt and send your documents directly from these applications.
- Decrypt only version of PrivateFile so that a recipient does not have to purchase a copy
- AES Encryption.
- A KeyStore to store your regularly used encryption keys.
- Simple Key Management – without the need to invest in a full PKI infrastructure.
- File and Document secure erasure.
- Easy to Use.



Technical Requirements:

• Operating System:	MS Windows 98/ME/NT/2000/XP
• Memory:	64MB
• Disk:	20MB

PrivateFile MailGateway



What is PrivateFile MailGateway?

PrivateFile MailGateway helps companies with their own email infrastructure, automatically protect their email attachments. It uses the *PrivateFile* encryption engine so that recipients can use their standard desktop *PrivateFile* application to decrypt. In addition it also integrates with PGP version 8.x so that email attachments can be sent PGP encrypted.

How it Works

PrivateFile MailGateway sits between your email client and the Internet. It scans any MIME emails with attachments as they pass through. Based on a set of rules which you can specify, it can automatically encrypt the attachments before passing the email on. The attachments are now encrypted and can be decrypted at the recipient end either by a corresponding copy of *PrivateFile MailGateway* or by a standard version of *PrivateFile*.

PrivateFile MailGateway can be configured to run as an external executable in *MailSweeper* or act as its own mail proxy (SMTP/POP3) using *PfMailProxy*, a companion product

Main Features:

- Encrypts/Decrypts email attachments based on a set of easy to setup rules
- Does not require a full PKI infrastructure
- Simple Key Management – using telephone or SMS
- *PrivateFile MailGateway Administrator* to setup/modify rules
- Integrates with existing email infrastructure either via an email management system such as *ClearSwift MailSweeper* or using *PfMailProxy*
- Uses *PrivateFile* encryption engine so compatible with standard desktop *PrivateFile* application.
- Works with PGP version 8.x, where PGP is installed
- Recipients can use a standard version of *PrivateFile* to decrypt the attachments.
- Administrator application to setup rules. Import/Export of rules based on CSV files

Technical Requirements:

• Operating System:	MS Windows NT 4/2000/XP
• Memory:	64MB
• Disk:	20MB
• Supported email format	MIME
• PGP support	Where PGP 8.x is installed

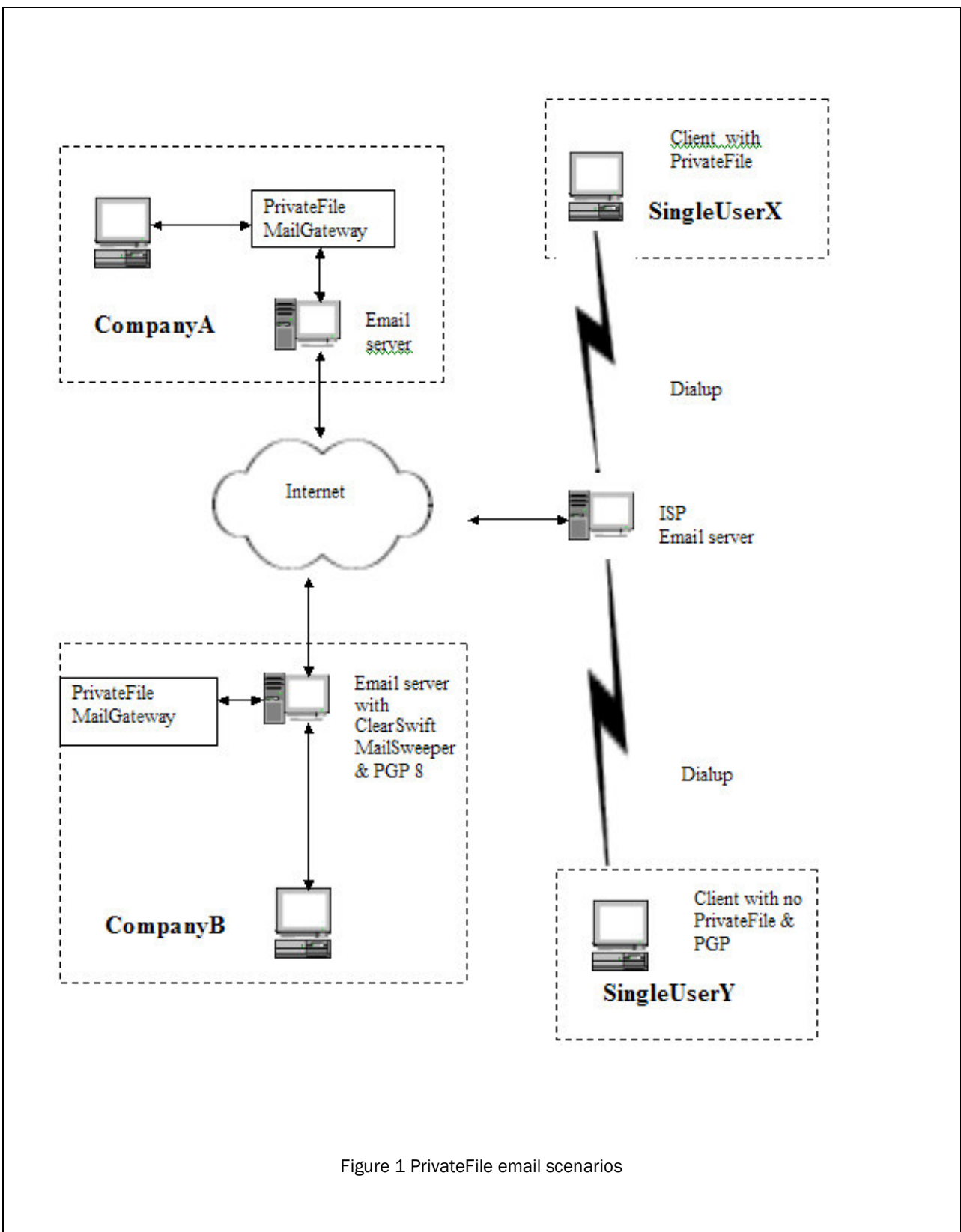


Figure 1 PrivateFile email scenarios

Configurations

Figure 1 shows a configuration where 4 parties want to exchange encrypted emails.

CompanyA has it's own email server for handling email (SMTP/POP3) traffic. In this case *PrivateFile MailGateway* can be inserted between each user's email client and the email server. The email client does not talk directly to the email server, but rather through *PrivateFile MailGateway*. This can then scan the email attachments and encrypt/decrypt them based on the rules that have been setup.

CompanyB already has an email scanning application such as ClearSwift's MailSweeper. In this case *PrivateFile MailGateway* is configured as an external executable which can be called from MailSweeper.

SingleUserX has a copy of *PrivateFile* installed and sends emails through an ISP.

SingleUserY has NO copy of *PrivateFile* installed and sends emails through an ISP.

Key Exchange between the various parties is done via simple out-of-band communications such as telephone or SMS text message. This is a simple alternative for those who do not want to invest in a full PKI infrastructure.

Scenarios

CompanyA – CompanyB

A rule is setup on CompanyA's *PrivateFile MailGateway* for sending to CompanyB. An equivalent rule is setup on CompanyB's *PrivateFile MailGateway* for receiving from CompanyA. When a user from CompanyA sends an email with an attachment to CompanyB, CompanyA's *PrivateFile MailGateway* will encrypt the email attachments using the rule. When the message arrives at CompanyB, it's *PrivateFile MailGateway* decrypts the attachments and forwards the email with the decrypted attachment onto the recipient.

CompanyA – SingleUserX

A rule is setup on CompanyA's *PrivateFile MailGateway* for sending to SingleUserX. When a user from CompanyA sends an email with an attachment to SingleUserX, CompanyA's *PrivateFile MailGateway* will encrypt the email using the rule. When the message arrives to SingleUserX, the user can use their standard copy of *PrivateFile* to decrypt the document.

CompanyA – SingleUserY

A rule is setup on CompanyA's *PrivateFile MailGateway* for sending to SingleUserY who does not have a copy of *PrivateFile*. This rule can specify that the attachments should be encrypted as a Self-Decrypting executable. When a user from CompanyA sends an email with an attachment to SingleUserY, CompanyA's *PrivateFile MailGateway* will encrypt the email using the rule. When the message arrives to SingleUserY, the user can decrypt the document using the Self-Decrypting executable. Alternatively the user can install the decrypt-only version of *PrivateFile*.

CompanyB – SingleUserY

A PGP rule is setup on CompanyB's *PrivateFile MailGateway* for SingleUserY. When a user from CompanyB sends an email with an attachment to SingleUserY, CompanyB's *PrivateFile MailGateway* will encrypt the email using the PGP rule. When the message arrives to SingleUserY, the user can decrypt the rule using their version of PGP.

PrivateFile MailGateway and PGP Version 8.x

PrivateFile MailGateway integrates with PGP version 8. PGP needs to be installed separately. It is not part of the *PrivateFile MailGateway* installation. If a rule is setup which matches the sender and recipient address and specifies that PGP be used, then any attachment is encrypted/decrypted using the PGP keyring.

For outbound messages, *PrivateFile MailGateway* uses the recipient's PGP public key to encrypt the attachments. For inbound messages, it uses the recipient's PGP private key to decrypt the attachments.

PrivateFile MailGateway Administrator

The user *PrivateFile MailGateway* Administrator application is used to setup the rules that *PrivateFile MailGateway* uses.

In the accompanying figure a rule has been setup so that when john.doe@companya.com sends an email with attachments to jane.smith@companyb.com, the attachments will be encrypted using *PrivateFile Standards*.

A message is appended to the bottom of the email giving information about the *PrivateFile* encryption.

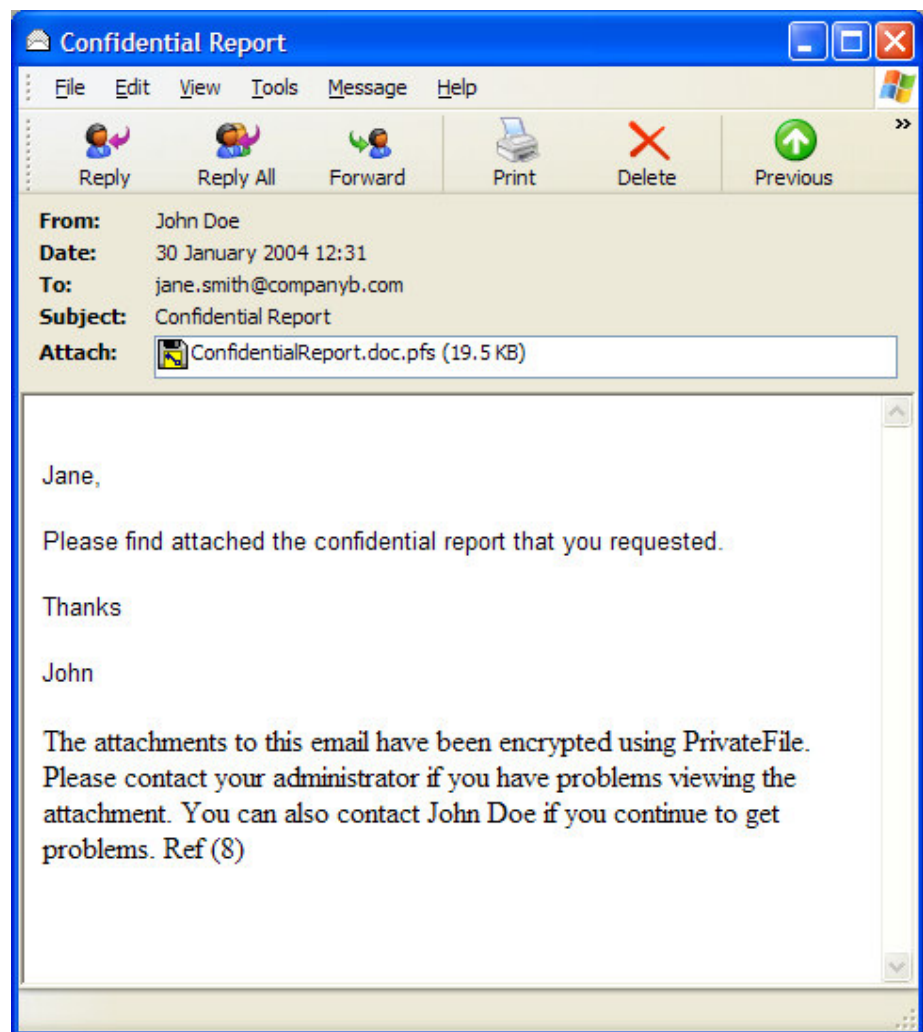
The screenshot shows a 'New Record' dialog box with the following fields and values:

ID	8
From Name	john.doe
From Domain	companya.com
To Name	jane.smith
To Domain	companyb.com
Key/PGP Passphrase	8kja434shkj127ss98d98asdf
Encryption Type	0 - PrivateFile Standard
In/Out	0 - Outbound
Allow Personal Encryption	<input type="checkbox"/>
Local Contact	Please contact your administrator if you have problems viewing the attachment.
Remote Contact	You can also contact John Doe if you continue to get problems
Multiple Recipients Rule ID	<input type="checkbox"/>
Fallback Rule ID	<input type="checkbox"/>

Buttons: OK, Cancel

This is a sample of an email with an attachment that John sent to Jane. Jane can use her copy of *PrivateFile* to decrypt the message.

A message has been appended to the bottom of the email containing more information.



PrivateFile Server



What is PrivateFile Server?

This is a component which you can integrate into your corporate applications to encrypt and protect files. These files can then be decrypted using PrivateFile Desktop.

<p>The component uses the underlying encryption engine (AES) as the other PrivateFile products. The simple API is exposed as a Windows COM component and can be called from VB, ASP, VBScript etc.</p>	<pre>key = "SecretKey" filename = "C:\confidentialReport.doc" iSelfDecrypt = 0 iZip = 1 rc = pf.SrvrEncryptFile(key, filename, iZip, iSelfDecrypt) If rc <> 0 Then message = pf.GetCurrentTask Else message = "Success!" End If</pre>
--	---

Main Features:

- Simple API
- Encrypt/Decrypt files
- Can be decrypted using PrivateFile Desktop
- Uses PrivateFile (AES) encryption engine
- Easily called from VB, VBScript etc.

Technical Requirements:

• Operating System:	MS Windows NT 4/2000/XP
• Memory:	64MB
• Disk:	20MB
• Development	VB, VBScript etc. Any language that supports COM

Contact:

Tel: +353-1-642 0550
Fax: +353-1-466 0468

Email: info@private-file.com
Web: www.private-file.com

Address PrivateFile Ltd.
2052 Citywest Digital Park,
Co. Dublin.
Ireland.