

External Recipients Encryption

Hermes SEG will send encrypted email to any external external recipient by by triggering the encryption though a keyword in an email subject (Please see **Encryption --> Encryption Settings** for more details) or by pre-configuring the external recipient for encryption. Triggering encryption by keyword in an email subject is certainly convenient but the problem with this approach is that it depends on the person sending the email to remember to enter the special keyword in the subject. If that person forgets to enter the keyword or misspells the keyword, the email will not be encrypted and potentially sensitive information can be compromised. For this reason, pre-configuring external recipients for encryption should be done whenever possible. On this page, you will be able to pre-configure external recipients for encryption as well as the type of encryption you wish to apply to each recipient.

Hermes SEG External Recipients Encryption are categorized in two categories: **Manual** and **Automatic** users. Manual users are external recipients that have been manually configured for encryption and automatic users are users that the system has automatically configured for encryption usually through the use of a subject trigger to send a PDF encrypted email to an external email address.

By default, a listing of **manually configured** external recipients will appear (assuming external recipients have been previously added) as evidenced by the **Show Manual Users Only** selection (**Figure 1**).

Figure 1

[Next 10 External Recipients >>](#)





































































































Recipient	Encryption Status				S/MIME Cert(s)			PGP Keyring(s)			Configure	PDF Passwd	Portal Passwd	Delete
Mr. John Doe john.doe@company.com	PDF No	PDF Mode N/A	S/MIME Mandatory	PGP No										
Ms. Jane Smith jane.smith@company.com	PDF No	PDF Mode N/A	S/MIME Mandatory	PGP No										
Mr. Robert Brown robert.brown@company.com	PDF No	PDF Mode N/A	S/MIME Mandatory	PGP No										
Ms. Emily White emily.white@company.com	PDF No	PDF Mode N/A	S/MIME Mandatory	PGP No										
Mr. David Green david.green@company.com	PDF No	PDF Mode N/A	S/MIME Mandatory	PGP No										
Ms. Sarah Black sarah.black@company.com	PDF No	PDF Mode N/A	S/MIME Mandatory	PGP No										
Mr. Michael Lee michael.lee@company.com	PDF No	PDF Mode N/A	S/MIME Mandatory	PGP No										
Ms. Lisa King lisa.king@company.com	PDF No	PDF Mode N/A	S/MIME Mandatory	PGP No										
Mr. James Hall james.hall@company.com	PDF No	PDF Mode N/A	S/MIME Mandatory	PGP No										
Ms. Karen Young karen.young@company.com	PDF No	PDF Mode N/A	S/MIME Mandatory	PGP No										

Figure 2

☐ Show Manual Users Only
 ☒ Show Automatic Users Only

Filter By
Set Filter
Clear Filter

[Next 10 External Recipients >>](#)

Displaying 1 through 10 out of 163 total external recipients

Recipient	Encryption Status			S/MIME Cert(s)		PGP Keyring(s)		Configure	PDF Passwd	Portal Passwd	Delete
Example Recipient 1	PDF	PDF Mode	S/MIME		+		+				
Example Recipient 2	No	N/A	No		+		+				
Example Recipient 3	PDF	PDF Mode	S/MIME		+		+				
Example Recipient 4	No	N/A	No		+		+				
Example Recipient 5	PDF	PDF Mode	S/MIME		+		+				
Example Recipient 6	No	N/A	No		+		+				
Example Recipient 7	PDF	PDF Mode	S/MIME		+		+				
Example Recipient 8	No	N/A	No		+		+				
Example Recipient 9	PDF	PDF Mode	S/MIME		+		+				
Example Recipient 10	No	N/A	No		+		+				

Create External Encryption Recipient

- On the **External Recipients Encryption** page, click on the **Create External Recipient** icon to create a new External Recipient. You will be re-directed to the **Create External Encrypted Recipient** page.
- On the **Create External Encrypted Recipient** page under the **Specify E-mail Address** field enter the address part on the field before the @ and the domain part after the @.
- Under the **Select Encryption Type** field, select the type of encryption you wish to use and click the **Continue** button (**Figure 3**).

Figure 3

Create External Encrypted Recipient

Specify E-Mail Address

@

Select Encryption Type

☒ Mandatory PDF Encryption
 ☐ PDF Encryption Triggered by E-mail Subject Keyword
 ☐ Mandatory S/MIME Encryption
 ☐ S/MIME Encryption Triggered by E-mail Subject Keyword
 ☐ Mandatory PGP Encryption
 ☐ PGP Encryption Triggered by E-mail Subject Keyword

Continue

- Mandatory PDF Encryption** - This will force ALL emails to that recipient to be encrypted utilizing PDF Encryption.

- **PDF Encryption Triggered by E-mail Subject Keyword** - This will only encrypt emails to the external recipient utilizing PDF encryption, ONLY if encryption is triggered by the e-mail subject keyword.
- **Mandatory S/MIME Encryption** - This will force ALL emails to that recipient to be encrypted utilizing S/MIME Encryption. Please note that a certificate must be created and/or imported for S/MIME encryption to work. If no certificate exists, all emails to that recipient will fail.
- **S/MIME Encryption Triggered by E-mail Subject Keyword** - This will only encrypt emails to that recipient utilizing S/MIME encryption ONLY if encryption is triggered by the e-mail subject keyword. Please note that a certificate must be created and/or imported for S/MIME encryption to work. If no certificate exists, any encrypted emails to that recipient will fail.
- **Mandatory PGP Encryption** - This will force ALL emails to that recipient to be encrypted utilizing PGP Encryption. Please note that a PGP Keystore must be created and/or imported for PGP encryption to work. If no PGP Keystore exists, all emails to that recipient will fail.
- **PGP Encryption Triggered by E-mail Subject Keyword** - This will only encrypt emails to that recipient utilizing PGP encryption ONLY if encryption is triggered by the e-mail subject keyword. Please note that a PGP Keystore must be created and/or imported for PGP encryption to work. If no PGP Keystore exists, all emails to that recipient will fail.

Configure External Encryption Recipient


1. On the **External Recipients Encryption** page, click on the  icon on an existing External Recipient to reconfigure encryption. You will be re-directed to the **Edit External Encrypted Recipient** page.
2. On the **Edit External Encrypted Recipient** page, under the **Select Encryption Type** field, select the type of encryption you wish to use and click the **Continue** button (**Figure 4**).

Figure 4

Edit External Encrypted Recipient

Specify E-Mail Address

someone@somedomain.tld

Select Encryption Type

- ☐ Mandatory PDF Encryption
- ☐ PDF Encryption Triggered by E-mail Subject Keyword
- ☐ Mandatory S/MIME Encryption
- ☒ S/MIME Encryption Triggered by E-mail Subject Keyword
- ☐ Mandatory PGP Encryption
- ☐ PGP Encryption Triggered by E-mail Subject Keyword

Continue

- **Mandatory PDF Encryption** - This will force ALL emails to that recipient to be encrypted utilizing PDF Encryption.

- **PDF Encryption Triggered by E-mail Subject Keyword** - This will only encrypt emails to the external recipient utilizing PDF encryption, ONLY if encryption is triggered by the e-mail subject keyword.
- **Mandatory S/MIME Encryption** - This will force ALL emails to that recipient to be encrypted utilizing S/MIME Encryption. Please note that a certificate must be created and/or imported for S/MIME encryption to work. If no certificate exists, all emails to that recipient will fail.
- **S/MIME Encryption Triggered by E-mail Subject Keyword** - This will only encrypt emails to that recipient utilizing S/MIME encryption ONLY if encryption is triggered by the e-mail subject keyword. Please note that a certificate must be created and/or imported for S/MIME encryption to work. If no certificate exists, any encrypted emails to that recipient will fail.
- **Mandatory PGP Encryption** - This will force ALL emails to that recipient to be encrypted utilizing PGP Encryption. Please note that a PGP Keystore must be created and/or imported for PGP encryption to work. If no PGP Keystore exists, all emails to that recipient will fail.
- **PGP Encryption Triggered by E-mail Subject Keyword** - This will only encrypt emails to that recipient utilizing PGP encryption ONLY if encryption is triggered by the e-mail subject keyword. Please note that a PGP Keystore must be created and/or imported for PGP encryption to work. If no PGP Keystore exists, all emails to that recipient will fail.

Mandatory PDF Encryption or PDF Encryption Triggered by E-mail Subject Keyword

Random Generated PDF Password through Secure E-mail Portal

Selecting this type of PDF encryption will configure the system to send encrypted PDF emails that will require the external recipient to access the Secure E-mail Portal and generate a random passwords that will then be used to open the encrypted PDF in order to read the email contents.

1. On the **Configure External Recipient PDF Encryption** page, select the **Random Generated PDF Password through Secure E-mail Portal** option.
2. Click the **Apply** button on the bottom of the page (**Figure 5**).

Figure 5

Configure External Recipient PDF Encryption

E-Mail Address

someone@somedomain.tld

Select PDF Encryption Type

- ☒ Random Generated PDF Password through Secure E-mail Portal (Recommended)
- ☐ Random Generated PDF Password Sent Back to Sender
- ☐ Specified PDF Password

PDF Password Age in Minutes (Ex: 60 = 1 Hour. Required when Back to Sender is selected. 15 Minutes Min)

60

PDF Password Length (Takes Effect Only when Back to Sender is selected)

- ☒ 160-Bits (Recommended)
- ☐ 128-bits

PDF Password (Required if Specified PDF Password selected. 8 characters, letters, numbers & special characters)

Verify PDF Password

Apply









- The **Apply** button will change to a **Please wait...** status (**Figure 6**).

Figure 6

Please wait...

- Once the system finishes configuring the external recipient encryption, it will redirect back to the **External Recipients Encryption** page (**Figure 7**). Note how the the **PDF Mode** under the **Encryption Status** column is set to **random**.

Figure 7

Recipient	Encryption Status				S/MIME Cert(s)	PGP Keyring(s)	Configure	PDF Passwd	Portal Passwd	Delete				
someone@somedomain.tld	PDF Mandatory	PDF Mode random	S/MIME No	PGP No										

✓ Success!! External Recipient Configured

Random Generated PDF Password Sent Back to Sender

Selecting this type of PDF encryption will configure the system to generate random password which will be emailed back to the sender of the email. The sender will in turn have to provide that random password to the external recipient in order the external recipient to open the encrypted PDF and read the email contents.

- On the **Configure External Recipient PDF Encryption** page, select the **Random Generated PDF Password Sent Back to Sender** option.
- Selecting the **Random Generated PDF Password Sent Back to Sender** option, will automatically enable the **PDF Password Age in Minutes** and the **PDF Password Length** fields.
- If needed, adjust the number of minutes under the **PDF Password Age In Minutes** field. This field sets the number of minutes the PDF password will be valid.

- If needed, adjust the **PDF Password Length** field. This field controls how long of a PDF password the system will generate. We recommend you leave it set to **160-Bits**.
- Click the **Apply** button on the bottom of the page (**Figure 8**).

Figure 8

Configure External Recipient PDF Encryption

E-Mail Address

Select PDF Encryption Type

☐ Random Generated PDF Password through Secure E-mail Portal (Recommended)
☒ Random Generated PDF Password Sent Back to Sender
☐ Specified PDF Password

PDF Password Age in Minutes (Ex: 60 = 1 Hour. Required when Back to Sender is selected. 15 Minutes Min)

PDF Password Length (Takes Effect Only when Back to Sender is selected)
☒ 160-Bits (Recommended)
☐ 128-bits

PDF Password (Required if Specified PDF Password selected. 8 characters, letters, numbers & special characters)

Verify PDF Password

- The **Apply** button will change to a **Please wait...** status (**Figure 9**).

Figure 9

- Once the system finishes configuring the external recipient encryption, it will redirect back to the **External Recipients Encryption** page (**Figure 10**). Note how the the **PDF Mode** under the **Encryption Status** column is set to **backtosender**.

Figure 10

Recipient	Encryption Status				S/MIME Cert(s)	PGP Keyring(s)	Configure	PDF Passwd	Portal Passwd	Delete
someone@somedomain.tld	PDF Mandatory	PDF Mode backtosender	S/MIME No	PGP No						

✓ Success!! External Recipient Configured

Specified PDF Password

Selecting this type of PDF encryption will configure the system to send encrypted PDF emails with a specified static password.

- On the **Configure External Recipient PDF Encryption** page, select the **Specified PDF Password** option.
- Selecting the **Specified PDF Password** option, will automatically enable the **PDF Password** and the **Verify PDF Password** fields.

3. Enter a password under the **PDF Password** field ensuring that it's at least 8 characters long and it includes letters, number and special characters.
4. Enter the password again under the **Verify PDF Password** field.
5. Click the **Apply** button on the bottom of the page (**Figure 11**).

Figure 11

Configure External Recipient PDF Encryption

E-Mail Address

someone@somedomain.tld

Select PDF Encryption Type

- ☐ Random Generated PDF Password through Secure E-mail Portal (Recommended)
☐ Random Generated PDF Password Sent Back to Sender
☒ Specified PDF Password

PDF Password Age in Minutes (Ex: 60 = 1 Hour. Required when Back to Sender is selected. 15 Minutes Min)

60

PDF Password Length (Takes Effect Only when Back to Sender is selected)

- ☒ 160-Bits (Recommended)
☐ 128-bits

PDF Password (Required if Specified PDF Password selected. 8 characters, letters, numbers & special characters)

Verify PDF Password

Apply

- The **Apply** button will change to a **Please wait...** status (**Figure 12**).

Figure 12

Please wait...

- Once the system finishes configuring the external recipient encryption, it will redirect back to the **External Recipients Encryption** page (**Figure 13**). Note how the the **PDF Mode** under the **Encryption Status** column is set to **static**.

Figure 13

Recipient	Encryption Status				S/MIME Cert(s)	PGP Keyring(s)	Configure	PDF Passwd	Portal Passwd	Delete
someone@somedomain.tld	PDF Mandatory	PDF Mode static	S/MIME No	PGP No						

✓ Success!! External Recipient Configured

Mandatory S/MIME Encryption or S/MIME Encryption Triggered by E-mail Subject Keyword

1. After clicking the Continue button the system does not ask any more questions as is the case with configuring PDF Encryption. It simply configures the External Recipient for either Mandatory S/MIME Encryption or S/MIME Encryption Triggered by E-mail Subject Keyword and re-directs back to the External Recipient Encryption page. Note that **S/MIME** under the **Encryption Status** column will be set to either **Mandatory** or **Subject** depending on the S/MIME encryption type you chose earlier (**Figure 14**).

Figure 14


Recipient	Encryption Status				S/MIME Cert(s)	PGP Keyring(s)	Configure	PDF Passwd	Portal Passwd	Delete
someone@somedomain.tld	PDF No	PDF Mode N/A	S/MIME Mandatory	PGP No	  	  				

 **Success!! External Recipient Configured**
 **You have selected S/MIME Encryption for this recipient. In order for S/MIME Encryption to work, you must create and/or import a S/MIME Certificate for this recipient**

2. As mentioned above, S/MIME encryption requires certificates to either be generated or imported. Please refer to the Generate External Recipient S/MIME Certificate or the Import External Recipient S/MIME Certificate sections below.

Generate External Recipient S/MIME Certificate

Do not attempt to generate a S/MIME Certificate for an External Recipient unless you have already enabled S/MIME encryption on that recipient.

1. Under the **S/MIME Certificate(s)** section of the External Recipient you wish to generate a certificate, click on the  icon.
2. You will be re-directed to the **Add Recipient S/MIME Certificate** page.
3. Assuming you have previously created an Internal Certificate Authority, under the **Certificate Authority** field, select the Internal Certificate Authority you wish to use to generate the S/MIME certificate.
4. Under the **S/MIME Certificate Validity Period**, select the number of years you wish this S/MIME Certificate to be valid. The default setting of 5 Years is recommended.
5. Under the **S/MIME Certificate Encryption Length**, select the length of the certificate. The default setting of 4096-bits is recommended.
6. Under the **S/MIME Certificate Algorithm**, select the algorithm you wish to generate the certificate. The default setting of RSA-SHA-512 is recommended.
7. Under the **Auto-Generate S/MIME Certificate and Private Key PFX password** field, select **Yes** to have the system automatically generate a password for the PFX file or select **No** if you wish to specify your own password. When generating a certificate, the system will also create a PFX file (Personal Information Exchange) and assign a password to it for security. A PFX file will contain both the public AND the private key of the generated certificate. The PFX file is used by the system for sending both the private and public key to the recipient that the certificate is being generated for for backup purposes

or for configuring an email client. It's recommended that you allow the system to generate a PFX file password.

- If you selected No in the **Auto-Generate S/MIME Certificate and Private Key PFX password**, enter the password you wish to use under the **S/MIME Certificate and Private Key PFX password** and enter the same password under the **Verify S/MIME Certificate and Private Key PFX password** field.
- Click on the **Create Certificate** button (**Figure 15**).

Figure 15

Add Recipient S/MIME Certificate

Internal Recipient

someone@somedomain.tld

Certificate Authority

Deeztek Root Certificate Authority ▼

S/MIME Certificate Validity Period

- ☒ 5 Years
☐ 4 Years
☐ 3 Years
☐ 2 Years
☐ 1 Year

S/MIME Certificate Encryption Length

- ☐ 2048-bits (medium security)
☒ 4096-bits (high security)

S/MIME Certificate Algorithm

- ☐ RSA-SHA-1 (least secure, most compatible)
☐ RSA-SHA-256 (mostly secure, mostly compatible)
☒ RSA-SHA-512 (most secure, least compatible)

Auto-Generate S/MIME Certificate and Private Key PFX password

- ☒ Yes (Recommended)
☐ No

S/MIME Certificate and Private Key PFX password

Verify S/MIME Certificate and Private Key PFX password

Create Certificate


- The system will generate the certificate and automatically redirect you back to the **External Recipients Encryption** page.
- Under the External Recipients listing on the S/MIME Certificate(s) section of the recipient you just generated a certificate, you will note the  icon which will now be enabled and clickable indicating that there are certificates present (**Figure 16**).

Figure 16

Recipient	Encryption Status				S/MIME Cert(s)	PGP Keyring(s)	Configure	PDF Passwd	Portal Passwd	Delete
someone@somedomain.tld	PDF No	PDF Mode N/A	S/MIME Mandatory	PGP No	 +	 +				

✓ Success!! External Recipient S/MIME Certificate created

Import External Recipient S/MIME Certificate

Do not attempt to import a S/MIME Certificate for an External Recipient unless you have already enabled S/MIME encryption on that recipient.

Hermes SEG ONLY supports importing S/MIME certificates from PFX (Personal Information Exchange) files. Ensure that you have a PFX file which will contain both the certificate and the private key along with the password of the PFX file before proceeding.


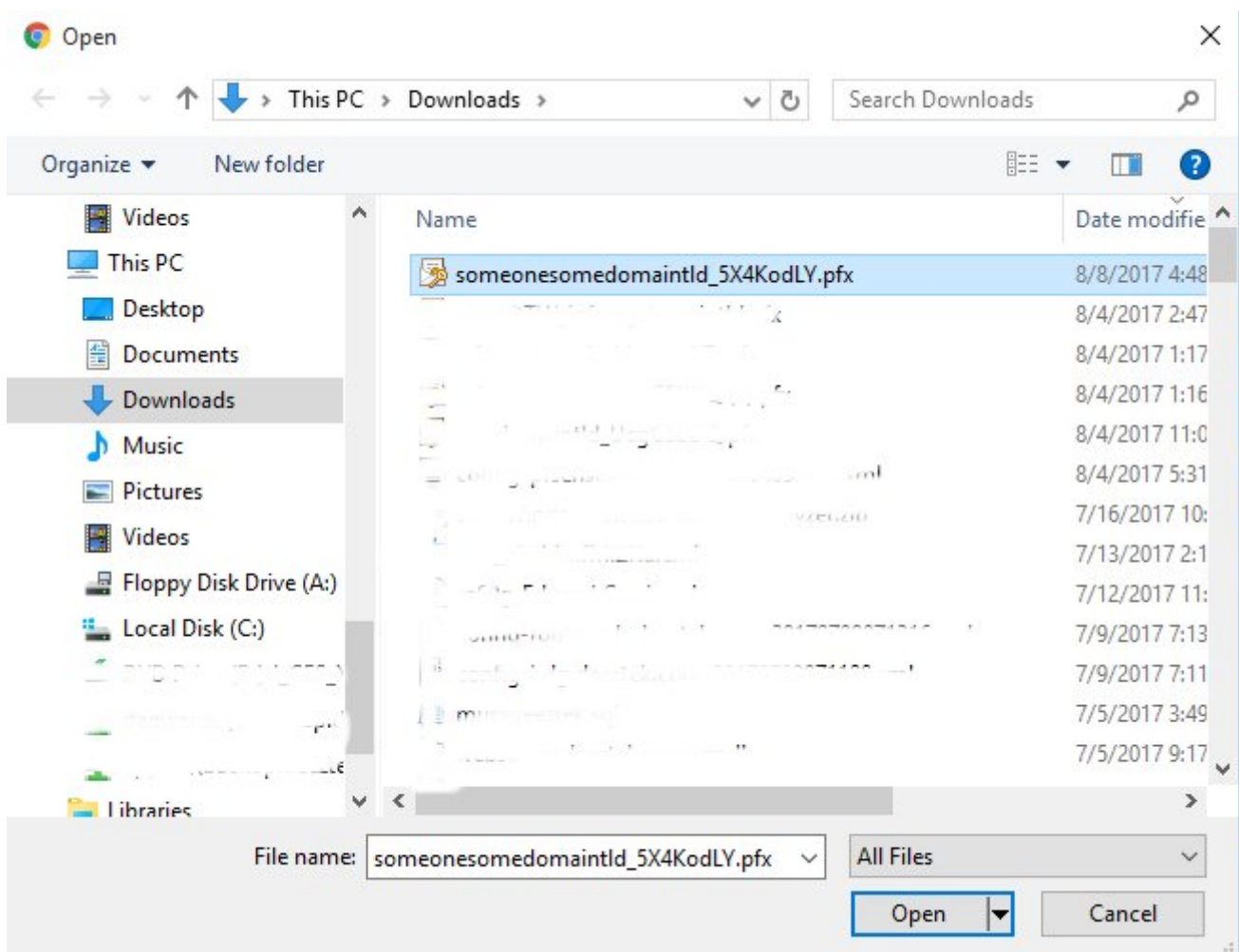
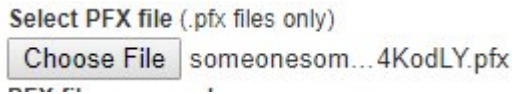
1. Under the **S/MIME Certificate(s)** section of the External Recipient you wish to import a certificate, click on the  icon.
2. You will be re-directed to the **Import Recipient S/MIME Certificate** page.
3. Under the **Select PFX File** section, click on the **Choose File** button.
4. Browse to the location of the PFX file, select the file and click the **Open** button (**Figure 17**).

Figure 17



5. The name of the PFX file you chose will appear next to the **Choose File** button (**Figure 18**).

Figure 18



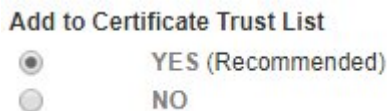
6. Under the **PFX file password** field, enter the password to the PFX file (**Figure 19**).

Figure 19



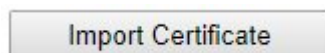
7. Under the **Add to Certificate Trust List** field, select **Yes** to add the certificate to the system Certificate Trust List. **Selecting Yes is always recommended** unless you have a specific reason not to trust the certificate you are importing. In that case, select No (**Figure 20**).

Figure 20



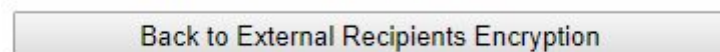
8. Click the **Import Certificate** button (**Figure 21**).

Figure 21



9. After a succesful import, click on the **Back to External Recipients Encryption** button on the bottom of the page (**Figure 22**).

Figure 22




10. Back at the **External Recipients Encryption** page, under the External Repients listing on the S/MIME Certificate(s) section of the recipient you just imported a certificate, you will note the  icon which will now be enabled and clickable indicating that there are certificates present (**Figure 23**).

Figure 23

Recipient	Encryption Status				S/MIME Cert(s)	PGP Keyring(s)	Configure	PDF Passwd	Portal Passwd	Delete
someone@somedomain.tld	PDF No	PDF Mode N/A	S/MIME Mandatory	PGP No	 +	 +				

✓ Success!! External Recipient S/MIME Certificate created

Download or Send PFX File

Hermes SEG will allow you to download or send to the External Recipient the password protected PFX file containing the certificate and private key.





1. At the **External Recipients Encryption** page, under the **S/MIME Certificate(s)** section, click on the  icon of the recipient you want to download or send the PFX file. You will be re-directed to the **View Recipient S/MIME Certificates** page (**Figure 24**).

Figure 24

View Recipient S/MIME Certificates

Recipient								
someone@somedomain.tld								
CA	Expires	Length	Algorithm	Delete	Download	Send		
	08/07/2022	4096 Bits	sha512					

Download PFX File

NEVER share PFX File passwords via unsecured means such as unencrypted email, SMS text etc.



1. Click on the  icon of the certificate you wish to download. Your browser will immediately start downloading the PFX file.
2. If you wish to view the PFX password, click on the  icon. You will be re-directed to the **Send Recipient PFX Certificate File & Password** page, where you will be able to view the PFX file password under the **PFX Certificate File Password** field (**Figure 25**).

Figure 25

Send Recipient PFX Certificate File & Password

The system will send the PFX Certificate File to the recipient via e-mail. The PFX Certificate File password is shown below in order to relay to the recipient. It is **HIGHLY** recommended that you do not relay the password via any communications medium including telephone, SMS or unencrypted e-mail. All those mediums are considered unsecure. Click the **Send Certificate** button below to proceed.

Recipient E-mail Address

PFX Certificate File Password

Send Certificate

Send PFX File

NEVER share PFX File passwords via unsecured means such as unencrypted email, SMS text etc.

Hermes SEG will send the PFX file ONLY to the recipient email address that the certiciate was generated/imported for.


1. Click on the  icon of the certificate you wish to send.
2. You will be re-directed to the **Send Recipient PFX Certificate File & Password** page.
3. Click on the **Send Certificate** button (**Figure 26**).

Figure 26

Send Recipient PFX Certificate File & Password

The system will send the PFX Certificate File to the recipient via e-mail. The PFX Certificate File password is shown below in order to relay to the recipient. It is **HIGHLY** recommended that you do not relay the password via any communications medium including telephone, SMS or unencrypted e-mail. All those mediums are considered unsecure. Click the **Send Certificate** button below to proceed.

Recipient E-mail Address

PFX Certificate File Password

4. If necessary, provide the password to the PFX file to the recipient via secured means.

Mandatory PGP Encryption or PGP Encryption Triggered by E-mail Subject Keyword

1. After clicking the Continue button the system does not ask any more questions as is the case with configuring PDF Encryption. It simply configures the External Recipient for either Mandatory PGP Encryption or PGP Encryption Triggered by E-mail Subject Keyword and re-directs back to the External Recipient Encryption page. Note that **PGP** under the **Encryption Status** column will be set to either **Mandatory** or **Subject** depending on the PGP encryption type you chose earlier (**Figure 27**).

Figure 27

Recipient	Encryption Status				S/MIME Cert(s)	PGP Keyring(s)	Configure	PDF Passwd	Portal Passwd	Delete
someone@somedomain.tld	PDF No	PDF Mode N/A	S/MIME No	PGP Mandatory		  				

2. As mentioned above, PGP encryption requires PGP Keystores to either be generated or imported. Please refer to the Generate External Recipient PGP Keystore or the Import External Recipient PGP Keystore sections below.

Generate External Recipient PGP Keyring

Do not attempt to generate a PGP Keyring for an External Recipient unless you have already enabled PGP encryption on that recipient.


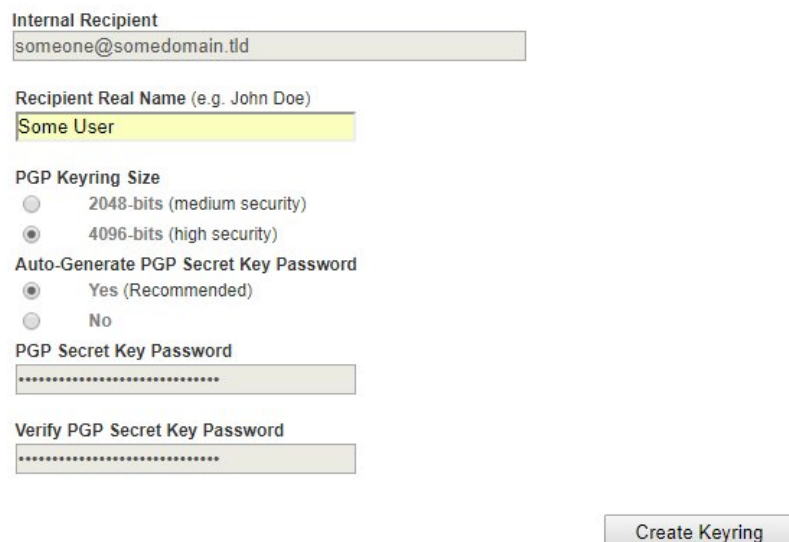
1. Under the **PGP Keyring(s)** section of the External Recipient you wish to generate a PGP Keyring, click on the .
2. You will be re-directed to the **Add Recipient PGP Keyring** page.
3. Under the **Recipient Real Name** section, enter the recipient's First and Last Name.
4. Under the **PGP Keyring Size**, select the size of the keyring. The default setting of 4096-bits is recommended.
5. Under the **Auto-Generate PGP Secret Key Password** field, select **Yes** to have the system automatically generate a password for the Secret Key or select **No** if you wish to specify your own password. It's recommended that you allow the system to generate a Secret Key password.
6. If you selected No in the **Auto-Generate PGP Secret Key password**, enter the password you wish to use under the **PGP Secret Key Password** and enter the same password under the **Verify PGP Secret Key Password** field below the first one.
7. Click on the **Create Keyring** button (**Figure 28**). Please note that clicking the **Create Keyring** button will not change the button status and the system may appear unresponsive. Please wait until the keyring get created and the system re-directs you back to the **External Recipients Encryption** page.

Figure 28

Add Recipient PGP Keyring



Internal Recipient
someone@somedomain.tld

Recipient Real Name (e.g. John Doe)
Some User


PGP Keyring Size
☐ 2048-bits (medium security)
☒ 4096-bits (high security)

Auto-Generate PGP Secret Key Password
☒ Yes (Recommended)
☐ No

PGP Secret Key Password









Verify PGP Secret Key Password

Create Keyring

10. The system will generate the keyring and automatically redirect you back to the **External Recipients Encryption** page.
11. Under the External Recipients listing on the **PGP Keyring(s)** section of the recipient you just generated a keystore, you will note the  icon which will now be enabled and

clickable indicating that there are keyrings present (**Figure 29**).

Figure 29

Recipient	Encryption Status				S/MIME Cert(s)	PGP Keyring(s)	Configure	PDF Passwd	Portal Passwd	Delete
someone@somedomain.tld	PDF No	PDF Mode N/A	S/MIME No	PGP Mandatory		  				

Import External Recipient PGP Keyring

Do not attempt to import a PGP Keyring for an External Recipient unless you have already enabled PGP encryption on that recipient.


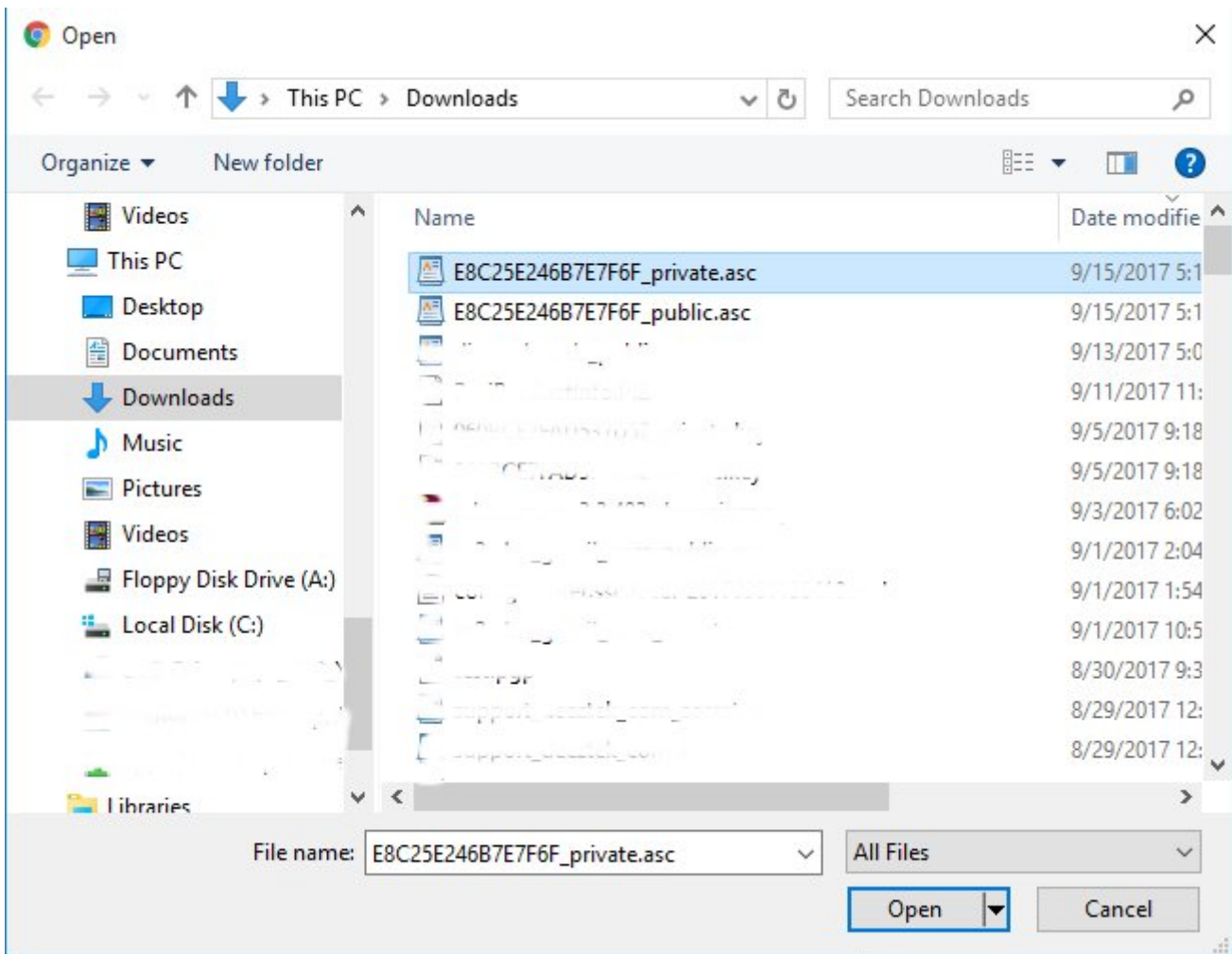
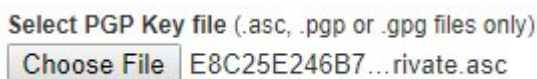
1. Under the **PGP Keystore(s)** section of the External Recipient you wish to import a keystore, click on the .
2. You will be re-directed to the **Import Recipient PGP Key** page.
3. Under the **PGP Key Type** field, select whether you will be importing a **Public** or a **Private** Key type. If you select a **Private** PGP Key Type, the **Private PGP Key Password** field below will become enabled.
4. If you selected a **Private** PGP Key Type above, enter the private key password in the **Private PGP Key Password** field.
5. Under the **Select PGP Key File** section, click on the **Choose File** button.
6. Browse to the location of the PGP key file, select the file and click the **Open** button (**Figure 30**).

Figure 30



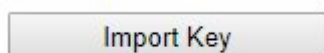
- The name of the PGP Key file you chose will appear next to the **Choose File** button (**Figure 31**).

Figure 31



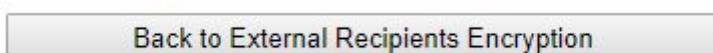
- Click the **Import Key** button (**Figure 32**).

Figure 32



- After a successful import, click on the **Back to External Recipients Encryption** button on the bottom of the page (**Figure 33**).

Figure 33











- Back at the **External Recipients Encryption** page, under the External Recipients listing on the **PGP Keyring(s)** section of the recipient you just imported a certificate, you will note the  icon which will now be enabled and clickable indicating that there are keystores present (**Figure 34**).

Figure 34

Recipient	Encryption Status				S/MIME Cert(s)	PGP Keyring(s)	Configure	PDF Passwd	Portal Passwd	Delete
someone@somedomain.tld	PDF No	PDF Mode N/A	S/MIME No	PGP Mandatory		 				

Delete Key, Download Public Key, Download Private Key, View Private Key Password and Publish Public Key


- At the **External Recipients Encryption** page, under the **PGP Keystore(s)** section, click on the  icon of the recipient. You will be re-directed to the **View Recipient PGP Keyrings** page (**Figure 35**).

Figure 35

View Recipient PGP Keyrings

Recipient someone@somedomain.tld												
Type	Size	User-ID	Created	Expires	Private Key	Key ID	Parent ID	Delete	Download Public	Download Private	View Password	Publish Key
MASTER	4096	Some User <someone@somedomain.tld>	09/16/2017	01/01/9999	Available	F43F736B99E4CDDF	N/A					
SUB	4096	Some User <someone@somedomain.tld>	09/16/2017	01/01/9999	Available	C7AE8531CA8AE93D F43F736B99E4CDDF						

Delete Key


- Click on the  icon of the key you wish to delete. You will be re-directed to the **Delete Recipient PGP Key** page (**Figure 36**).

Figure 36

Delete Recipient PGP Key

The system will delete the PGP Key indicated below. Deleting a key is **irreversible**. If you are deleting a **Master PGP Key**, the system will automatically delete any associated **Sub Keys**. If you delete the last Key for a PGP enabled recipient, PGP encryption will no longer work until you generate or import another PGP Keyring for this recipient. If you are sure you wish to delete this key, click the **Delete Key** button. Otherwise, click on the **Back to Recipient PGP Keyrings** button.

Recipient
someone@somedomain.tld

Type	Size	Name	Created	Expires	Private Key	Key ID	Parent ID
MASTER	4096	Some User	09/16/2017	01/01/9999	Not Available	F43F738B99E4CDDF	N/A

Delete Key

Back to Recipient PGP Keyrings

2. Click the **Delete** Key button. Please note that if you are deleting the **Master** Key, the system will automatically delete both the Master and any associated Sub Keys. If you are deleting a **Sub** Key, the system will only delete the Sub Key you selected to delete. If you wish to cancel, click on the **Back to Recipient PGP Keyrings** button.
3. Clicking the **Delete** button will delete the key and re-direct you back to the **External Recipients Encryption** page (Figure 37).

Figure 37

Recipient	Encryption Status				S/MIME Cert(s)	PGP Keyring(s)	Configure	PDF Passwd	Portal Passwd	Delete
someone@somedomain.tld	PDF No	PDF Mode N/A	S/MIME No	PGP Mandatory						

Success!! External Recipient PGP Key deleted

Download Public Key or Private Key

Downloading the Public and Private Keys is useful for importing those keys in 3rd party PGP applications such as Enigma, Kleopatra etc.

1. Click on the icon under the **Download Public** or the **Download Private** column of the key you wish to download. Your browser will automatically begin downloading the key you clicked in **ASCII armor** format.

View Private Key Password

This feature is useful in determining the **Private Key** password that the system automatically generates when generating a PGP Keyring. **NEVER** share **Private Key** passwords via unsecured means such as unencrypted email, SMS text etc.

1. Click on the icon under the **View Password** column of the key you wish to view the private key password.
2. You will be re-directed to the **View Recipient PGP Private Key** Password page (Figure 38).

[View Recipient PGP Private Key Password](#)

Recipient E-mail Address

PGP Private Key Password

[Back to Recipient PGP Keyrings](#)

Please note that if no PGP Key Servers are defined under **Encryption** --> **PGP Key Servers** the icons under the Publish Key column of every key will be disabled .

- ### Publish Recipient Public PGP Key

Recipient

PGP Key ID

4ED985EEF6267536

Select All

None

Publish Key

[Back to Recipient PGP Keyrings](#)

- Created 3 January 2021 15:38:47 by Dino Edwards

