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 mispells 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 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**).

Filter By Set Filter Clear Filter

Next 10 External Recipients >>

Displaying 1 through 10 out of 33 total external recipients

Recipient		Encrypt	tion Statu	s	S/M	IME Ce	ert(s)	PGP	Keyri	ng(s)	Configure	PDF Passwd	Portal Passwd	Delete
· · · · · · · · · · · · · · · · · · ·	PDF No	PDF Mode N/A	S/MIME Mandatory	PGP No	-	+	7	R	÷	Y	×	-		×
daan juuri	PDF No	PDF Mode N/A	S/MIME Mandatory	PGP No		+	7	R	₽		×			×
	PDF No	PDF Mode N/A	S/MIME Mandatory	PGP No	1	+	7	R	+	7	×			×
card R	PDF No	PDF Mode N/A	S/MIME Mandatory	PGP No	-	+	Y	R	+	Y	×			×
·	PDF No	PDF Mode N/A	S/MIME Mandatory	PGP		+	Y	R	+	7	×	-		×
C	PDF No	PDF Mode N/A	S/MIME Mandatory	PGP	1	+	Y	R	₽	7	×	-		×
more	PDF No	PDF Mode N/A	S/MIME Mandatory	PGP No		+	7	R	₽	7	×			×
63	PDF No	PDF Mode N/A	S/MIME Mandatory	PGP No		₽	Y	R	÷	7	×	-		×
6	PDF No	PDF Mode N/A	S/MIME Mandatory	PGP No		+	Y	M	÷	7	×	-		×
e •	PDF No	PDF Mode N/A	S/MIME Mandatory	PGP No		-	7	R	÷	7	×	-		×

If you wish to view the **automatically configured** external recipients, select the **Show Automatic Users Only** selection (**Figure 2**).

\bigcirc	Show Manual Users Only	۲	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	En	cryption	Status	S/MI	ME C	ert(s)	PGP	Keyri	ng(s)	Configure	PDF Passwd	Portal Passwd	Delete
	PDF No	PDF Mode	S/MIME No		÷	7	R	÷	7	×		•	×
Resource Control of the	PDF No	PDF Mode	S/MIME No		÷	7	M	÷	Y	×		•	×
	PDF No	PDF Mode N/A	S/MIME No		₽	7	R	₽	7	×	-		×
te la Mar Seconda en est	PDF No	PDF Mode N/A	S/MIME No		÷	Y	R	÷	Y	×		•	×
ຕາວນັ້ງມູມີໄດ້ເຫັງ	PDF No	PDF Mode N/A	S/MIME No	•=	÷	Y	R	₽	Y	×		•	×
مروح المعرفين المروح	PDF No	PDF Mode	S/MIME No		÷	7	M	₽	Y	×		•	×
146.5	PDF No	PDF Mode N/A	S/MIME No		₽	7	R	÷	7	×		•	×
s _ Interaction and weather a final sector	PDF No	PDF Mode N/A	S/MIME No		÷	Y	R	÷	Y	×			×
sjanoos e egan ros	PDF No	PDF Mode N/A	S/MIME No	ŧ=	÷	7	R	÷	Y	×	-		×
The sector of th	PDF No	PDF Mode	S/MIME No		₽	7	R	₽	Y	×	-		×

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.
- 2. 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 @.
- 3. Under the **Select Encryption Type** field, select the type of encryption you wish to use and click the **Continue** button (**Figure 3**).

Figure 3

Crea Speci	te External Encrypted Recipient
	@
Selec	t Encryption Type
۲	Mandatory PDF Encryption
0	PDF Encryption Triggered by E-mail Subject Keyword
0	Mandatory S/MIME Encryption
0	S/MIME Encryption Triggered by E-mail Subject Keyword
0	Mandatory PGP Encryption
0	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 email 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 Kicon on an existing External Recipient to reconfigure encryption. You will be re-directed to the **Edit External Encrypted Recipient** page.
- 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

Speci	ify E-Mail Address	
some	eone@somedomain.tld	
Selec	t Encryption Type	
0	Mandatory PDF Encryption	
\odot	PDF Encryption Triggered by E-mail Subject I	Keyword
0	Mandatory S/MIME Encryption	
۲	S/MIME Encryption Triggered by E-mail Subje	ct Keyword
0	Mandatory PGP Encryption	
\bigcirc	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 email subject keyword.
- **Mandatory S/MIME Encryption** This will force ALL emails to that recipeint 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 recipeint 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**).

someo	ne@somedomain.tld
Select I	PDF Encryption Type
۲	Random Generated PDF Password through Secure E-mail Portal (Recommended)
0	Random Generated PDF Password Sent Back to Sender
0	Specified PDF Password
PDF Pa	ssword Age in Minutes (Ex: 60 = 1 Hour. Required when Back to Sender is selected. 15 Minutes Min)
60	
PDF Pa	460 Bits (Pacommanded)
PDF Pa	160-Bits (Recommended) 128-bits ssword (Required if Specified PDF Password selected. 8 characters, letters, numbers & special characters
PDF Pa	160-Bits (Recommended) 128-bits ssword (Required if Specified PDF Password selected. 8 characters, letters, numbers & special characters DF Password
PDF Par	Ssword Length (Takes Ellect Only When Back to Sender is selected) 160-Bits (Recommended) 128-bits ssword (Required if Specified PDF Password selected. 8 characters, letters, numbers & special characters DF Password
PDF Pa	Ssword Length (Taxes Ellect Only when Back to Sender is selected) 160-Bits (Recommended) 128-bits ssword (Required if Specified PDF Password selected. 8 characters, letters, numbers & special characters DF Password

• 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	E	ncryption	Status		S/M	IME Ce	ert(s)	PGP	Keyri	ng(s)	Configure	PDF Passwd	Portal Passwd	Delete
someone@somedomain.tld	PDF Mandatory	PDF Mode random	S/MIME No	PGP No		÷	7	R	÷	Y	×		<u>_</u>	×

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.

- 1. 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.
- 3. 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.

- 4. 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**.
- 5. Click the **Apply** button on the bottom of the page (**Figure 8**).

Figure 8

someo	ne@somedomain.tld
Select F	PDF Encryption Type
0	Random Generated PDF Password through Secure E-mail Portal (Recommended)
۲	Random Generated PDF Password Sent Back to Sender
0	Specified PDF Password
PDF Pas	ssword Age in Minutes (Ex: 60 = 1 Hour. Required when Back to Sender is selected. 15 Minutes Min)
60	ne or the standard standard for an and the standard standard and the second standard standard based
PDF Pas	ssword Length (Takes Effect Only when Back to Sender is selected) 160-Bits (Recommended)
PDF Pas	ssword Length (Takes Effect Only when Back to Sender is selected) 160-Bits (Recommended)
PDF Pas	ssword Length (Takes Effect Only when Back to Sender is selected) 160-Bits (Recommended) 128-bits ssword (Required if Specified PDF Password selected, 8 characters, letters, numbers & special characters
PDF Pas	ssword Length (Takes Effect Only when Back to Sender is selected) 160-Bits (Recommended) 128-bits ssword (Required if Specified PDF Password selected. 8 characters, letters, numbers & special characters
PDF Pas	ssword Length (Takes Effect Only when Back to Sender is selected) 160-Bits (Recommended) 128-bits ssword (Required if Specified PDF Password selected. 8 characters, letters, numbers & special characters
PDF Pas	ssword Length (Takes Effect Only when Back to Sender is selected) 160-Bits (Recommended) 128-bits ssword (Required if Specified PDF Password selected. 8 characters, letters, numbers & special characters DF Password
PDF Pas PDF Pas Verify P	ssword Length (Takes Effect Only when Back to Sender is selected) 160-Bits (Recommended) 128-bits ssword (Required if Specified PDF Password selected. 8 characters, letters, numbers & special characters DF Password
PDF Pas PDF Pas Verify P	ssword Length (Takes Effect Only when Back to Sender is selected) 160-Bits (Recommended) 128-bits ssword (Required if Specified PDF Password selected. 8 characters, letters, numbers & special characters DF 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	E	Encryption	Status		S/M	IME Ce	ert(s)	PGP	Keyri	ng(s)	Configure	PDF Passwd	Portal Passwd	Delete
someone@somedomain.tld	PDF Mandatory	PDF Mode backtosender	S/MIME No	PGP No		÷	Y	R	÷	Ľ	×	-	•	×
Success!! External Recipier	nt Configured	1												

Specified PDF Password

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

- 1. On the **Configure External Recipient PDF Encryption** page, select the **Specified PDF Password** option.
- 2. 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 leters, 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

	ne@somedomain.tld
Select F	PDF Encryption Type
0	Random Generated PDF Password through Secure E-mail Portal (Recommended)
0	Random Generated PDF Password Sent Back to Sender
۲	Specified PDF Password
PDF Pa	ssword Age in Minutes (Ex: 60 = 1 Hour. Required when Back to Sender is selected. 15 Minutes Min)
60	
PDF Pas	160-Bits (Recommended) 128-bits ssword (Required if Specified PDF Password selected. 8 characters, letters, numbers & special characters)
	•
Verify P	DF Password

• 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	E	ncryption	Status		S/M	IME Ce	ert(s)	PGP	Keyri	ing(s)	Configure	PDF Passwd	Portal Passwd	Delete
someone@somedomain.tld	PDF Mandatory	PDF Mode static	S/MIME No	PGP No		÷	Y	R	÷	Y	×	-	•	×
Success!! External Recipien	t Configured													

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

 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



2. As mentioned above, S/MIME encryption requires certificates to either be generated or imported. Please refer to the Generate External Recipient S/MIME Certicate 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.
- 9. Click on the **Create Certificate** button (**Figure 15**).

Figure 15

Add Recipient S/MIME Certificate

memo	al Recipient
some	one@somedomain.tld
Certif	cate Authority
Deez	tek Root Certificate Authority 🔻
S/MIM	E Certificate Validity Period
۲	5 Years
0	4 Years
0	3 Years
0	2 Years
0	1 Year
S/MIM	E Certificate Encryption Length
0	2048-bits (medium security)
۲	4096-bits (high security)
S/MIN	E Certificate Algorithm
0	RSA-SHA-1 (least secure, most compatible)
0	RSA-SHA-256 (mostly secure, mostly compatible)
۲	RSA-SHA-512 (most secure, least compatible)
Auto-	Generate S/MIME Certificate and Private Key PFX password
۲	Yes (Recommended)
0	No
S/MIM	E Certificate and Private Key PFX password
	•••••

Create Certificate

- 10. The system will generate the certificate and automatically redirect you back to the **External Recipients Encryption** page.
- 11. 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**).

Recipient		Encryp	tion Statu	s	S/MIN	NE Ce	rt(s)	PGP	Keyri	ing(s)	Configure	PDF Passwd	Portal Passwd	Delete
someone@somedomain.tld	PDF No	PDF Mode N/A	S/MIME Mandatory	PGP No		-	7	R	÷	Y	×	-		×
Success!! External Recipier	t S/MIME	Certificat	e 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).

→ This PC	> Downloads > V C Search Downloads	,
rganize 🔻 New folder		- 🔳 (
Videos ^	Name	Date modif
💻 This PC	someonesomedomaintId_5X4KodLY.pfx	8/8/2017 4:
🔜 Desktop	- A A A A A A A A A A A A A A A A A A A	8/4/2017 2:
Documents		8/4/2017 1:
🕹 Downloads		8/4/2017 1:
h Music		8/4/2017 11
Pictures	= colling president and and	8/4/2017 5:
Videos	Section Vection	7/16/2017 1
		7/13/2017 2
Floppy Disk Drive (A:)		7/12/2017 1
Local Disk (C:)	VIII0-100 1 1 1 1 1 2017070071010 1	7/9/2017 7:
	¹ configure de la companya de la compa	7/9/2017 7:
The second se	[] muraleenek og	7/5/2017 3:
	7	7/5/2017 9:
Libraries Y	<	:
File name:	omeonesomedomaintId 5X4KodLY.pfx V All Files	,

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

Figure 18

Select PFX file (.pfx files only) Choose File someonesom...4KodLY.pfx

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

Figure 19

PFX file password	

 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

Add to Certificate Trust List

۲	YES (Recommended)
0	NO

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

Figure 21

Import Certificate

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

Figure 22

Back to External Recipients Encryption

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**).



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 click 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

	someone@somedomain	Recipient .tld				
CA	Expires	Length	Algorithm	Delete	Download	Send
	08/07/2022	4096 Bits	sha512	×	+	4

Download PFX File

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

- 1. Click on the vicon of the certificate you wish to download. Your browser will immediately start downloading the PFX file.
- 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 recommended that <u>you do not relay the passworr</u> unsecure. Click the Send Certificate button below t	recipient via e-mail. The PFX Certificate File password is shown below in order to relay to the recipient. It is <u>HIGHLY</u> 1 via any communications medium including telephone, SMS or unencrypted e-mail. All those mediums are considered o proceed.
Recipient E-mail Address	
someone@somedomain.tld	
PFX Certificate File Password	
Kcjh14EeFHPy2v5N	
	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 $\frac{4}{2}$ 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 re recommended that <u>you do not relay the password</u> unsecure. Click the Send Certificate button below to	ecipient via e-mail. The PFX Certificate File password is shown below in order to relay to the recipient. It is <u>HIGHLY</u> via any communications medium including telephone, SMS or unencrypted e-mail. All those mediums are considered proceed.
Recipient E-mail Address	
someone@somedomain.tld	
PFX Certificate File Password	
Kcjh14EeFHPy2v5N	
	Send Certificate

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

 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 redirects 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		Encryptic	on Statu	IS	S/M	IME Ce	rt(s)	PGP	Keyriı	ng(s)	Configure	PDF Passwd	Portal Passwd	Delete
someone@somedomain.tld	PDF No	PDF Mode N/A	S/MIME No	PGP Mandatory	•=	÷	Y	R	÷	Y	×	-	•	×

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 **PGP** icon.
- 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 4096bits is recommended.
- 5. Under the **Auto-Generate PGP Secret Key Password** field, select **Yes** to have the systtem 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 Seccret 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

Intern	al Recipient
some	one@somedomain.tld
Recip	ient Real Name (e.g. John Doe)
Some	e User
PGP I	Keyring Size
0	2048-bits (medium security)
۲	4096-bits (high security)
Auto-	Generate PGP Secret Key Password
۲	Yes (Recommended)
0	No
PGP	Secret Key Password
	DCD Count Key Doorwood
verity	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 *recipient will now be enabled and*

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

Figure 29

Recipient		Encrypti	on Stat	us	S/M	IME Ce	ert(s)	PGP	Keyrir	ng(s)	Configure	PDF Passwd	Portal Passwd	Delete
someone@somedomain.tld	PDF No	PDF Mode N/A	S/MIME No	PGP Mandatory	() ()	÷	Y	//	₯	Y	×	-		×

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 **N**icon.
- 2. You will be re-directed to the **Import Recipient PGP Key** page.
- 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.
- Browse to the location of the PGP key file, select the file and click the **Open** button (Figure 30).

Organize New folder Videos	lana		
Videos ^ r	1		
This DC	vame		Date modifie
This PC	E8C25E246B7E7F6F_private.asc		9/15/2017 5:
E Desktop	E8C25E246B7E7F6F_public.asc		9/15/2017 5:
🖆 Documents			9/13/2017 5:
🕹 Downloads	<u> </u>		9/11/2017 1
b Music	$\sum_{i=1}^{n} \left(OE(h_{i}) + (-h_{i}) + (\sigma_{i}, (\rho_{i})) \right)^{-1} \right) = \left(- \frac{1}{2} + \frac$		9/5/2017 9:1
			9/5/2017 9:1
Videos	-		9/3/2017 6:0
			9/1/2017 2:0
Floppy Disk Drive (A:)	<u>=,</u> ,		9/1/2017 1:5
Local Disk (C:)			9/1/2017 10:
· · · · · · · · · · · · · · · · · · ·	* rar		8/30/2017 9:
- The second sec			8/29/2017 12
	العجيد فيتعدد والمعالية والمعالية		8/29/2017 12
📜 Libraries 🗸 🗸 🗸			>
File name: E8C2	5E246B7E7F6F_private.asc	✓ All Files	~

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

Figure 31

Select PGP Key file (.asc, .pgp or .gpg files only)
Choose File E8C25E246B7...rivate.asc

6. Click the Import Key button (Figure 32).

Figure 32



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

Figure 33

Back to External Recipients Encryption

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

Figure 34

Recipient		Encrypti	on Stati	us	S/M	IIME Ce	ert(s)	PGP Key	ring(s)	Configure	PDF Passwd	Portal Passwd	Delete
someone@somedomain.tld	PDF No	PDF Mode N/A	S/MIME No	PGP Mandatory		÷	Y		7	×	-		×

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 recipient. You will be re-directed to the View Recipient PGP Keyrings page (Figure 35).

Figure 35

View Recipient PGP Keyrings

						Recipient						
				someone	@somed	omain.tld						
Туре	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></someone@somedomain.tld>	09/16/2017	01/01/9999	Available	F43F736B99E4CDDF	N/A	×	+			6
SUB	4096	Some User <someone@somedomain.tld></someone@somedomain.tld>	09/16/2017	01/01/9999	Available	C7AE8531CA8AE93D F	43F736B99E4CDDF	×		-		0

Delete Key

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

Delete Recipient PGP Key

			some	eone@somedomain	.tld		
Туре	Size	Name	Created	Expires	Private Key	Key ID	Parent ID
MASTER	4096	Some User	09/16/2017	01/01/9999	Not Available	F43F736B99E4CDDF	N/A
				Delete	Key		

- 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		Encrypti	on State	us	S/M	IME Ce	ert(s)	PGP	Кеугі	ng(s)	Configure	PDF Passwd	Portal Passwd	Delete
someone@somedomain.tld	PDF No	PDF Mode N/A	S/MIME No	PGP Mandatory		÷	Y	R	÷	Y	×			×
Success!! External Recipien	t PGP Ke	v 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 **J**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 con under the **View Password** column of the key you wish to view the private key password.
- You will be re-directed to the View Recipient PGP Private Key Password page (Figure 38).

Figure 38

View Recipient PGP Private Key Password

Ine PGP Private Key password is shown below in order including telephone, SMS or unencrypted e-mail. All the Recipient E-mail Address	to relay to the recipient. It is HIGHLY recommended that you do not relay, the password via any communications medium e mediums are considered unsecure.
someone@somedomain.tld	
PGP Private Key Password	
PTu1cQn5n+w gt ctrim distance and	
	Back to Recipient PGP Kevrings

Publish Public PGP Key

This feature is helpful with publishing recipient Public PGP Keys to Public PGP Key Servers. Public PGP Key Servers act as central repositories for public keys in order to assist in PGP cryptography.



- 1. Click on the $^{(1)}$ icon under the **Publish Key** column of the key you wish to publish.
- 2. You will be re-directed to the **Publish Recipient PGP Public Key** page (Figure 39).

Figure 39

Publish Recipient Public PGP Key

The system will publish the PGP Public Key indicated below to any PGP Key Servers you select. By default, the system automatically selects all the PGP Key Servers in the inventory. If you wish to only publish to selected servers, select only the servers you wish to publish to below and click the Publish Key button. Once finished, click on the Back to Recipient PGP Keyrings button.

		Necipient	
		someone@somedomain.tld	
		PGP Key ID	
		4ED985EEF6267536	
elect All	None		
Select	Key Server		Note
	ha.pool.sks-keyservers.net	Ot	enPGP SKS Key Server High Availability
	keyserver.ubuntu.com	U	buntu SKS OpenPGP Public Key Server
		Publish Key	
		Back to Recipient PGP Keyrings	

- By default all the configured Public PGP Key Servers are selected. If desired, uncheck any key servers from the list that you do not wish to publish the public key and click the **Publish Key** button.
- 4. When finished, click, on the **Back to Recipient PGP Keyrings** button on the bottom of the page.

Updated 2 December 2021 12:47:24 by Dino Edwards