PGP Secure Email (S/MIME) Guide for External Organisations

Version date: 20/07/2012
Status: Final
Contents

CONTENTS ........................................................................................................................................... 2

1. GLOSSARY OF TERMS ..................................................................................................................... 3

2. INTRODUCTION ............................................................................................................................... 4

3. OVERVIEW ....................................................................................................................................... 4

4. ENCRYPTION TECHNOLOGIES USED BY DWP ............................................................................. 5
   4.1 MIME (used as the encoding standard for OpenPGP) ................................................................. 5
   4.2 S/MIME ........................................................................................................................................ 5

5. WHAT DO EXTERNAL ORGANISATIONS NEED TO HAVE IN PLACE? ........................................ 5

6. RECEIVING WHOLLY ENCRYPTED MESSAGES - BOUNDARY ISSUES ......................................... 6
   6.1 ANTI VIRUS SCANNING ............................................................................................................... 6
   6.2 DLP (DATA LOSS PREVENTION) ................................................................................................ 6

7. INSTRUCTIONS FOR PGP DESKTOP PRO AND PGP UNIVERSAL USERS ............................... 7
   7.1 HOW WILL A NEW DWP KEY BE SENT? ..................................................................................... 7
   7.2 EXTRACTING A CERTIFICATE FROM A DWP XSIGN’ED EMAIL .............................................. 8
   7.3 IMPORTING TO YOUR PGP DESKTOP PRO/PGP UNIVERSAL LOCAL KEY STORE ..................... 9
   7.4 ONCE THE X.509 CERTIFICATE HAS BEEN IMPORTED ............................................................ 9

8. INSTRUCTIONS FOR USERS USING MICROSOFT OUTLOOK AS THEIR ENCRYPTION TOOL ...... 10
   8.1 SETTING UP YOUR OWN LOCAL TRUSTED KEY ....................................................................... 10
   8.2 RECEIVING A DIGITALLY SIGNED EMAIL FROM YOUR DWP COUNTERPART AND TRUSTING THEIR PUBLIC KEY ............................................................. 10
   8.3 SENDING BACK A SIGNED EMAIL WITH YOUR PUBLIC KEY EMBEDDED .................................. 13

9. FURTHER INFORMATION .................................................................................................................. 14
## 1. Glossary of Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digitally Signed Email</td>
<td>A digital signature is not visible to the sender. When you receive a digitally signed Email it will display a visual cue for the Digital Signature, i.e. a red rosette (which is specific to MS Outlook) or a yellow icon. A light blue banner shows that the message has been signed by an OpenPGP key. A digital signature means that the body of a message cannot be altered without invalidating the digital signature. The recipient can therefore verify that the message originated from the person whose signature is attached and has not been altered since it was signed.</td>
</tr>
<tr>
<td>Key</td>
<td>A key is a piece of information (sometimes called a crypto variable digital code) that is used in conjunction with an algorithm or cipher to encrypt, sign, decrypt and verify information. In modern systems it is often stored digitally as a string of a particular size. Keys can be either: Symmetric – The same key is used for encryption and decryption; Asymmetric – Different, linked keys are used for encryption and decryption operations.</td>
</tr>
<tr>
<td>Key Pair</td>
<td>A ‘Key Pair’ refers to a Public Key and its corresponding Private Key. One key, termed ‘Public’ is designed to be shared without compromising security, while the ‘Private’ key MUST be kept in a secure manner ensuring it is not disclosed to anyone.</td>
</tr>
<tr>
<td>PGP</td>
<td>Pretty Good Privacy is now a trademark of Symantec Corporation, however it is used colloquially to refer to the OpenPGP secure email standard.</td>
</tr>
<tr>
<td>Public Key</td>
<td>The Public Key (contained in an x.509 or OpenPGP digital certificate) is used primarily for encryption and is shared with external organisations with which data exchange is required. The Public Key in isolation does not allow decryption of any data; however it does provide a mechanism for the identification of a message’s sender.</td>
</tr>
<tr>
<td>Private Key</td>
<td>The Private Key is used to decrypt data and, by the signer, in digital signing operations. Unlike the Public Key which can be shared, the Private Key must be kept secure.</td>
</tr>
<tr>
<td>XCRYPT</td>
<td>Inclusion of XCRYPT in the subject line of any externally bound mail from DWP will send the Email in an encrypted &amp; signed format. The Email subject line is not encrypted.</td>
</tr>
<tr>
<td>XSIGN</td>
<td>Inclusion of XSIGN in the subject line of any externally bound mail from DWP will send the Email digitally signed. Digitally signed guarantees that the Email content has not been altered since the Email was sent.</td>
</tr>
</tbody>
</table>
2. Introduction

The DWP has introduced a service which supports the use of encryption to provide confidentiality, integrity and authenticity for email communications. This guide provides information on the technologies used and some basic checks that can be made to ensure your environment is configured to support secure email communication with DWP.

This guidance is provided on a current ‘as is’ basis. It is not possible for DWP to comment on the implementations of the individual mail solutions used by external organisations with whom DWP correspond.

3. Overview

In the past, the Department for Work and Pensions (DWP) has encrypted files using the Public Key of external organisations utilising PGP Desktop Pro software (the encryption format was PGP/MIME). These encrypted files were then attached to outbound emails sent to the intended recipient. On receipt the external organisation then decrypted the attachment using the Private portion of their PGP Key Pair.

The DWP has recently expanded their encryption capability and can wholly encrypt outbound emails at the gateway to an external organisation in either the desktop based OpenPGP (MIME) encryption format (which the existing DWP PGP Desktop Pro service utilises) or to a gateway based S/MIME V3 format, dependant on the recipients preferred format.

The DWP can also decrypt inbound emails in both S/MIME v3 and OpenPGP formats.

New DWP Public Keys will be created and will be forwarded to external organisations in the form of either a X.509 Digital Certificate or an OpenPGP Key. These certificate files should then be imported into the external organisation’s encryption service to allow future encryption of files/email using the recipient’s Public Key. Please ensure that the corresponding existing DWP Public Key is replaced.

An external organisation can supply the Public Keys of their users to the DWP in either format (OpenPGP Key or an S/MIME Key in the form of a X.509 Certificate) and they will be uploaded and stored on the DWP PGP Universal Server.
4. Encryption Technologies used by DWP

The DWP have introduced a dual-key configuration which allows the DWP to receive encrypted content in either MIME (OpenPGP) or S/MIME V3 formats.

4.1 MIME (used as the encoding standard for OpenPGP)

MIME (Multipurpose Internet Mail Extensions) is an Internet standard for describing the contents of a message. MIME is a standard for encoding information, and MIME messages can contain text, images, audio, video, and other application-specific data, rather than just plain text messages.

For the purpose of the DWP Secure Email service, OpenPGP keys will be provided to external organisations that utilise OpenPGP for secure communication. The preferred encoding format for DWP secure email using OpenPGP will be PGP MIME.

4.2 S/MIME

S/MIME (Secure / Multipurpose Internet Mail Extensions) is an internet standard that supports the encryption and digital signing of Emails and attachments such that their transport is protected and their origin is assured.

In practice they utilise a standard MIME message (the format of all internet based Emails) to ensure compliance but add attachments which hold either the encrypted message body (a *.p7m attachment) or the digital signature (a *.p7s attachment).

For the purpose of the DWP Secure Email service the X.509 certificates will be provided to external organisations that do not have PGP products in place.

5. What do external organisations need to have in place?

In order to send digitally signed emails, or receive encrypted emails, you need to have your own digital Key Pair that has been either self signed, or signed by a Certificate Authority (CA) for greater assurance. This Key Pair must have associated with it the email address you wish to use.

This should be supplied and signed by your company/organisation, but can be signed by independent trusted third-party CA’s such as Verisign, at a small additional cost.

Please Note: A Key Pair is specific to your email address and therefore should match the email address that you use for this communication, e.g. if you have a certificate issued from “company.com” then it will not work with an “organisation.com” email account.

External organisations will be able to utilise existing encryption software that they currently have in place as long as the software supports the standards noted in section 4.
In order to read DWP wholly encrypted emails there may be a requirement for some organisations utilising PGP Desktop Pro to amend the license to include the ‘Messaging’ component. This component supports the decryption of wholly encrypted content.

PGP Universal Server Gateway Email has the functionality in place to encrypt, decrypt and sign encrypted email messages.

Some organisations only send encrypted data attachments to the DWP and do not receive any encrypted content from the DWP. Although this is acceptable it is recommended that these organisations add the ‘Messaging’ component as follows:

- Open PGP desktop
- Click PGP messaging on the left
- Ensure your key is selected as the default key
- Then Click messaging at the top of the screen
- Click enable service

6. Receiving wholly encrypted messages - Boundary Issues

The most common considerations for organisations receiving wholly encrypted or signed emails are as follows.

6.1 Anti Virus scanning

Encryption often means that Anti Virus products are not able to scan the content of incoming messages; it may trigger a policy to remove the attachment from the message.

As the attachment is either the digital signature or the encrypted body, this can render the mail unreadable.

Any scanning should permit the encrypted content from DWP and other organisations to pass. Once it has been decrypted, there is then an opportunity to scan for malware.

6.2 DLP (Data Loss Prevention)

As above, the messages cannot be scanned by Data Loss Prevention products (by their nature this is more likely to occur on outbound messages), therefore any policies should be checked to ensure they do not block or tamper with the message in any way. DLP is generally not an issue on ingress of email into the environment, however outbound this can cause issues. DLP scanning, if used, should inspect and make a decision before encryption takes place. This is easier to implement with a gateway mail encryption solution.
7. Instructions for PGP Desktop Pro and PGP Universal users

7.1 How will a new DWP Key be sent?

Digitally Signed Email

The DWP user will send a standard Email with XSIGN in the subject field. This Email will have a X.509 Certificate embedded into it. This will be in the form of a digital signature. In practice this will show as a Rosette or a Yellow icon at the right of the Email header, however if PGP Desktop Pro is running these symbols may not be displayed.

Note: If PGP services are running then your Email client may not register the attached certificate as being valid and will not allow you to process it. Please stop your PGP Desktop Pro services from running. To do this right click on the padlock icon in the system tray (bottom right of the screen).

This will display a menu.
Please select ‘Stop/Exit PGP Services’.

A PGP Alert dialogue box will appear. Please select the ‘Yes’ option.

![PGP Alert](image)

If your organisation uses Lotus Notes this Digital Certificate may be handled differently. If you are a Lotus Notes user please refer to your local support area for advice and instruction for extracting the X.509 Certificate from the digitally signed email.

### 7.2 Extracting a Certificate from a DWP XSIGN’ed email

If you are using a Microsoft Outlook as your email product please follow the instructions below. These are generic instructions for extracting the X.509 Certificate in Microsoft Outlook and as such some of the references may be slightly different.

This process shouldn’t take long to complete.

Remember that PGP services should not be running whilst you carry out these steps otherwise you may not see the Rosette/Yellow icon.

1. Click on the Rosette or the Yellow icon at the right hand side of the email header.
2. Click on the ‘Details’ button. This will open the Message Security Properties dialogue box.
3. Click on the ‘View Details’ button. This will open the Signature dialogue box.
4. Click on the ‘View Certificate…’ button. This will open the View Certificate dialogue box.
5. Click on the Details tab and select the ‘Copy to File…’ button. This will open the Certificate Export Wizard.
6. Click on the ‘Next’ button.
7. Ensure the DER encoded binary X.509 (.CER) option is selected as the format to use and click on the ‘Next’ button.
8. On the next screen click on the ‘Browse…’ button.
9. Select a destination to save the file in, enter a name in the File Name field e.g. Joe Smith DWP Certificate and click on the ‘Save’ button.
10. The file path will then be displayed. Check and click on the ‘Next’ button.
11. On the next screen click on the ‘Finish’ button, this will give a confirmation box showing that the export is complete.

The X.509 Certificate is now extracted and stored ready for import into your PGP Desktop Pro/PGP Universal local Keystore. An overview of this process is included in the next section.

Remember: If you are using Lotus Notes please contact your local support for advice on extracting the X.509 Certificate from the digitally signed email.

7.3 Importing to your PGP Desktop Pro/PGP Universal Local Key Store

In order to import the newly extracted certificate into your PGP Desktop Pro/PGP Universal Local Key Store, please follow the steps below. This process shouldn’t take long to complete:

1. Open PGP via the ‘START’ Menu.
2. Click on File along the top Menu Bar and navigate to ‘Import…’ This will open ‘Select File Containing Key’ box.
3. Select the location where the exported certificate from the above section was saved and highlight the certificate file.
4. Highlight the file and click the ‘Open’ button.
5. This will open the Select Key(s) dialogue box. Highlight the certificate and click on the ‘Import’ button.
6. This will import the new certificate and will appear in your PGP Desktop Pro/PGP Universal Local Key Store ready for use.

7.4 Once the X.509 Certificate has been imported

When the Certificate has been imported to your PGP Desktop Pro/PGP Universal Local Key Store, it is worth testing to ensure a secure transfer is established. Once the secure transfer route can be confirmed it can be utilised on an ongoing basis.
8. Instructions for users using Microsoft Outlook as their encryption tool

8.1 Setting up your own local trusted key

When you have your Key Pair (this will be in a standard format e.g. .CER) it needs to be imported into your local desktop key store.

It is important that you keep your Private Key private. If you undertake a key exchange then this should be the exchange of the Public Key only.

This is automatically taken into account if you facilitate the key exchange using signed emails in line with item 2 below. However, this needs to be understood if you export the key from your keystore to send manually.

When your key has been supplied to you, it needs to be imported from within the Internet Options menu – Content tab, Certificates button and be displayed in your Personal certificate store.

(The following screenshots are based on Microsoft Outlook, other email clients may differ however they should have similar capabilities).

8.2 Receiving a digitally signed email from your DWP counterpart and trusting their Public Key

To be able to send you a signed email your DWP counterpart must include a keyword of XSIGN in the email subject line.

When you first receive an XSIGN email, your DWP counterpart’s digital signature, i.e., Public Key, will show up as invalid.
Double-Click on the red exclamation mark in the golden diamond 🔄. This will open up the certificate settings.

The Details button will bring up the certificate properties. Click on the “Signer:” email address and then “Edit Trust”.

This will allow you to view the certificate and bring up the trust editing screen.

You then need to explicitly trust the certificate from that email address and then click OK.

From then on, the email will show a red rosette 🏵️ every time you receive a valid signed email from that user.
The key for that DWP user is now configured in Outlook.
8.3 Sending back a signed email with your Public Key embedded

Your Public Key now needs to now be sent back to the DWP user.

Click “REPLY” on the original XSIGN message, then click on the Email Options and alter the Security Settings.

This will allow you to tick the boxes to say if the email is to be signed or encrypted.

Tick the box to sign the email to complete the key exchange.
Once the key exchange is complete and the DWP user has received your key and trusted it using the DWP Key Management Service (DWP users do this in PGP Universal, not in the Outlook client) they will send you an encrypted email by including a keyword of XCRYPT in the email subject line.

Successful encryption will be indicated by a padlock 🛠 next to the rosette.

You need to respond to the email by sending an encrypted reply to verify that communication both ways has been successful.

9. Further Information
Further information can be found from your own IT support function or from publicly available knowledgebase’s e.g. the Microsoft Outlook support pages: http://office.microsoft.com/en-us/outlook/HP012305371033.aspx