BANK OF ENGLAND

Secure Email User Guide

Transport Layer Security (TLS)

Pretty Good Privacy (PGP)

PDF Messenger

BANK OF ENGLAND

Contents

BANK OF ENGLAND

1 Introduction

The Bank of England's secure email policy

The Bank of England takes the security and integrity of email communication very seriously. Using a secure email solution provides an added layer of protection to minimise the risk of interception and misuse of confidential information.

The Bank of England's information security policy states that confidential electronic information exchanged with external counterparties / reporting institutions must be encrypted.

The Bank of England supports three secure email solutions:

Transport Layer Security (TLS) guarantees encrypted gateway to gateway delivery of all email between two organisations. In order to work, TLS needs to be enabled on the mail servers of both the sender and the receiver of the email. All information exchanged between the servers is then encrypted.

Pretty Good Privacy (PGP) is used to encrypt and decrypt email over the Internet. It uses digital keys (a public key/private key pair), that allow the receiver to verify the sender's identity and the integrity of the message. PGP has been used by the Bank of England for a number of years, and while it will continue to be supported for the foreseeable future, the Bank of England's preferred secure email solution going forward is TLS.

PDF Messenger delivers email and attachments to your mailbox as a PDF document, which is opened by entering a password. No special encryption software is required, you only need Adobe Acrobat Reader version 7 installed on your computer.

BANK OF ENGLAND

2 Transport Layer Security (TLS)

What is TLS?

Transport Layer Security (TLS) is a mail server feature which, once enabled, guarantees encrypted gateway to gateway delivery of all email between two organisations.

In order to work, TLS needs to be enabled on the mail servers of both the sender and the receiver of the email. This then creates a secure connection between the two organisations and all information exchanged between the servers is encrypted.

What are the advantages of TLS?

- It is a very user-friendly solution — there are no training requirements and any complexity is hidden from the end-user.
- All email exchanged between the Bank of England and external organisations enrolled onto TLS will be encrypted, removing the risk of email being inadvertently sent without encryption.
- Once set up, ongoing support and maintenance costs are low.
- It allows incoming email to be scanned for viruses or malicious content.
- It is straightforward to deploy, and requires configuration of email servers rather than set up of individual users.
- Email is delivered direct to your corporate mailbox.
- You can save both the email content and any attachments to your computer or document library without encryption.
- Where appropriate to do so, users are able to forward the email.

What are the disadvantages of TLS?

- Your email server will need to be configured to use TLS.

Do I need special software to receive email via TLS?

The Bank of England's standard for the use of TLS is 'enforced TLS', whereby the server is configured to force all email to be sent securely. If your email infrastructure does not currently support enforced TLS or meet the TLS cipher suite recommendations, you may need to purchase new software and/or infrastructure. (See FAQs for details.)

If your firm uses an external supplier to manage your email, you may require an arrangement with them.

Are there any costs associated with this option?

If your email servers are not configured for enforced TLS there may be initial set-up costs for your firm for the configuration of your email server. There are no charges from the Bank of England to exchange encrypted email but there may be charges from your email provider.

3 Pretty Good Privacy (PGP)

What is PGP?

Pretty Good Privacy (PGP) enables end-point to end-point encryption and decryption of email sent over the Internet. It uses digital keys (a public key/private key pair), that allow the receiver to verify the sender's identity and the integrity of the message.

What are the advantages of PGP?

- Emails and attachments are encrypted and protected when in transit between sender and receiver.
- Emails are sent and received from your corporate mailbox, so once set up the solution is easy to use.
- Where appropriate to do so, users are able to forward the email as long as the recipient is also set up to receive email by PGP.

What are the disadvantages of PGP?

- All PGP users need to be set up individually, and this will generally require IT support.
- PGP is licensed per user.
- Encrypted email cannot be scanned for viruses or malicious content.
- Keys are required to be set up and exchanged in advance of any secure communication.

Do I need special software to receive email using PGP?

Yes, a PGP licence is required for each PGP user.

Are there any costs associated with this option?

To enrol your firm onto PGP, you will need to buy a PGP Desktop licence for each user. The licences are available from any Symantec Authorised Reseller, and cost approximately £150 per user per year.

4 PDF Messenger

What is PDF Messenger?

PDF Messenger allows delivery of email and attachments from the Bank of England to your corporate mailbox as a PDF document, which is then opened using a user defined private password.

What are the advantages of PDF Messenger?

• There is no need for special encryption software — you only need Adobe Acrobat Reader version 7 and Internet Explorer version 6 or higher.
• Emails and attachments are encrypted and protected when in transit between sender and receiver.
• Email from the Bank of England is delivered to your corporate mailbox whereas other similar solutions require you to log into a web portal to access the message.
• Emails and attachments from the Bank of England can be saved locally to your computer or document library.

What are the disadvantages of PDF Messenger?

• You cannot forward PDF Messenger emails. This would require you to share your private password and this cannot be removed.
• Should you wish to use the 'secure reply' facility or compose a new email to the Bank of England using this solution, the communication takes place within the Bank of England's secure environment and therefore you cannot save these emails locally.
• Certain attachment types such as ZIP and EXE are not compatible with this solution.
• There is a file attachment limit of 20MB per email and an overall mailbox limit of 50MB.
• Encrypted email cannot be scanned for viruses or malicious content.

Do I need special software to receive email using PDF Messenger?

No special encryption software or licence is required but you will need Adobe Acrobat Reader version 7 and Internet Explorer version 6 or higher. There is a one-off registration process when you first use the service, which will require you to choose a private username and password. Once you have completed the initial registration process, encrypted PDF Messenger email messages will be sent directly to your mailbox.

Are there any costs associated with this option?

There is no cost for PDF Messenger.

4.1 Further PGP Information:

The PGP Gateway provides two solutions for reporting institutions to exchange secure emails with the Bank of England.

- PGP Web Messenger – emails are sent and received via a secure web browser interface.
- Using PGP Software at your institution and exchanging keys with the Bank.

The table below will help you decide which of the two PGP options is best for you – you may need to speak with your IT support staff to decide.

SOLUTION	USE IF	AND
PGP Web Messenger	You don't have a PGP key	You don't want or you are unable to install PGP software
PGP Software	You have a PGP key	You currently use PGP software or are willing to purchase

5 PGP Web Messenger

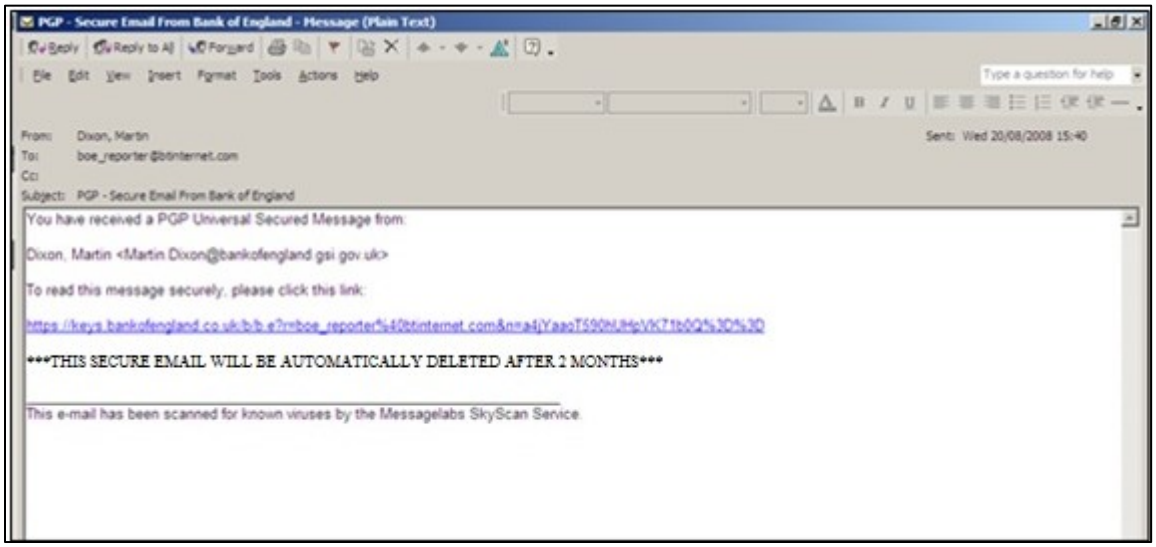
There is no need to purchase or install any software to use PGP Web Messenger. PGP Web Messenger is a web based mail client used to secure your communication with the Bank of England. It also allows you to send email messages and attachments securely to any email address at the Bank. Please note that non secure messages will continue to be sent to you by normal email.

The PGP Web Messenger ONLY permits sending of mail to Bank of England addresses. Mail addressed within the Web Messenger portal to NON-Bank of England recipients will NOT be transmitted or received. Please ensure you have taken appropriate steps to ensure non-Bank of England recipients have visibility of your correspondence.

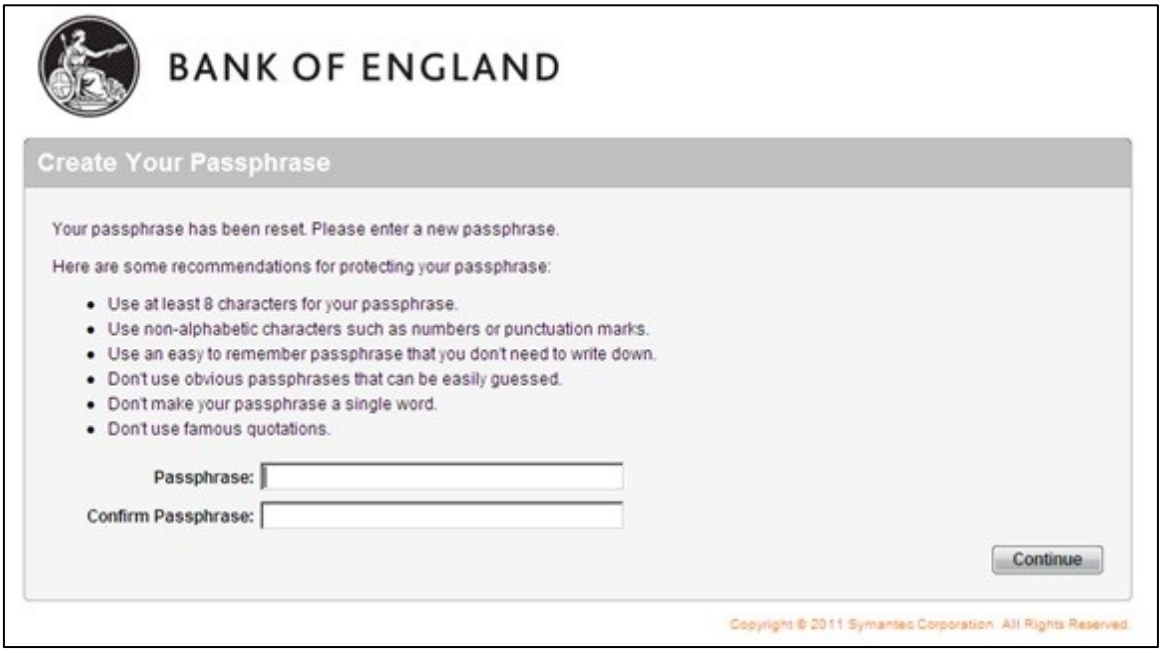
PGP Web Messenger is intended to be used as a secure method of transferring sensitive information via email, and not as a storage or archive space. There is a 50MB size limit for your secure Inbox and messages stored in your secure Inbox are automatically removed from the server after 2 months. You should save a copy of the information received via PGP Web Messenger locally. Inactive PGP Web Messenger accounts are automatically deleted after 6 months.

6 Enrolling as a PGP Web Messenger User

The first step is to enrol on the Bank of England PGP Web Messenger system by requesting the Bank to create you a PGP account. The enrolment process will be triggered when your account has been made active by the Bank, and you receive an e-mail from another PGP user. This first e-mail you receive will prompt you to click on a link and create a passphrase. This happens once and provides a secure email account for each enrolled user.



Click the link, and you will be prompted to create a passphrase.



Enter your passphrase twice (in both the **Passphrase** and **Confirm Passphrase** fields) and select the **Continue** button.

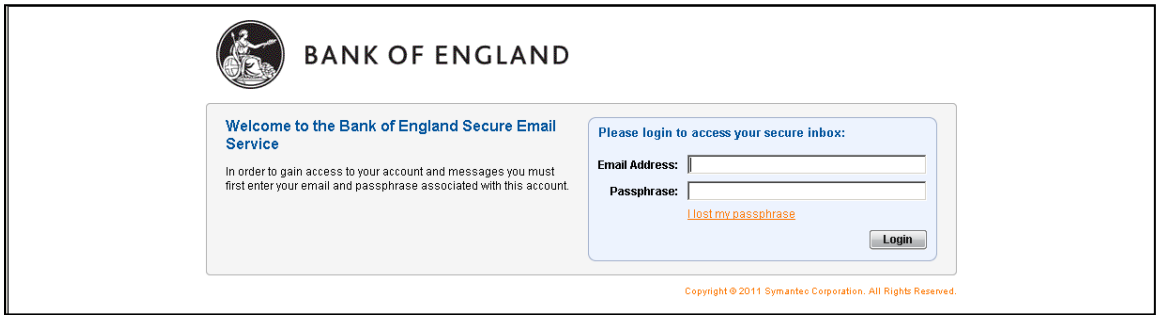
You will see the Message Delivery Options window appear (as illustrated below)

- Select the **PGP Universal Web Messenger** radio button
- Select **Choose Option**
- Your PGP Web Messenger mailbox will now appear.

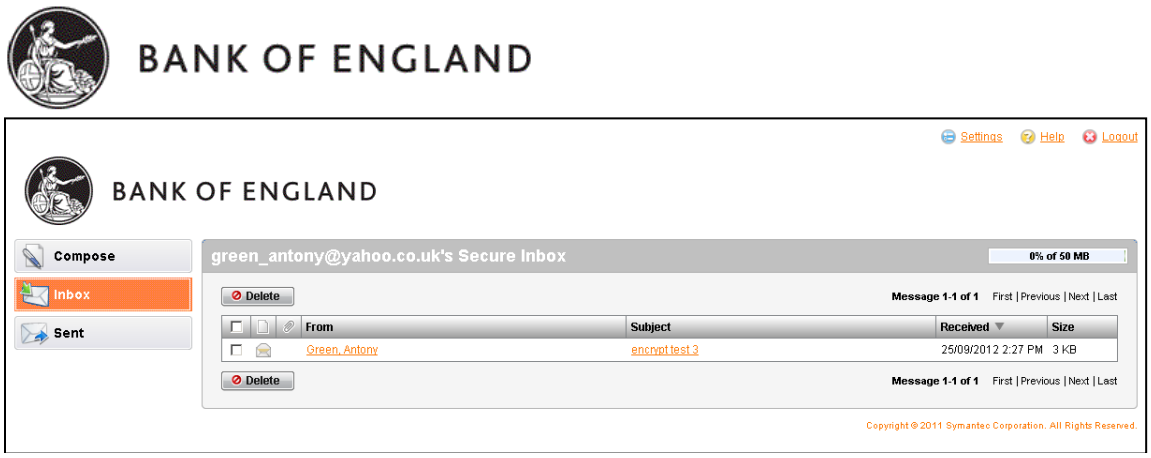
7 How to use PGP Web Messenger

7.1 Mailbox access

Once you have enrolled to access your mailbox browse to https://keys.bankofengland.co.uk and enter your email address and your passphrase.



Your mailbox will be displayed.



7.2 Send a Message

- Click the **Compose** button
- In the **To**: field

  Type in the email address of the person to whom you want to send a message

Note: When you compose a message remember that you can use this interface to send secure email messages to Bank of England email addresses only. Email to other addresses will be rejected

- In the **Subject**: field

  Type in a subject for your message

  Type your message into the text box under the subject

  When you are finished:
- Click the **Send** button

Note: It is not possible to

.1 *Present PGP Web Messenger users with Bank of England Global Address List that offers the Bank staff email contacts to be selected when composing a new mail. This is by design. Alternatively you can simply copy and paste the Bank staff email address from you Outlook contacts list.*

.2 *To receive a non-delivery report*

.3 *To receive read receipts*

7.3 Attach an attachment to a message

- Select **Add attachment**

  The Attachments dialog appears. You can browse to find files to attach.
- Select Attach
- Select OK

Note: The Bank of England will not allow email which contains the disallowed content. For example

.1 Executables: Executables can be released on request by your business contact. These could be released if the email is expected and only if the email and attachment are business related.

.2 Profanity: Message body or attachments contain a profanity.

.3 Multimedia: Emails that contain multimedia (MP3, WAV etc.) content or an inappropriate image.

7.4 Cancel a Message

If you decide you do not want to send the message you have been writing

- Click **Cancel**

7.5 Send a Message to multiple recipients

- Click the **Compose** button
- In the **To**: field

  Add more than one email address or CC: field

To add another email address after the first

- Type a comma or a semicolon after the first email address and then type in the next address

7.6 Read a Message

From your **Inbox**

- Select the message you want to read.

To return to the list of messages

- Select **Inbox**

To check for new messages

- Select **Inbox**

Note: There is a 50MB size limit for your secure Inbox and messages stored in your secure Inbox are automatically removed from the server after 2 months. You should save a copy of the information received via PGP Web Messenger localy.

7.7 Delete a Message

- Select the check box next to the message you want to delete.
- Select **Delete**

Note: It is not possible to retrieve deleted messages.

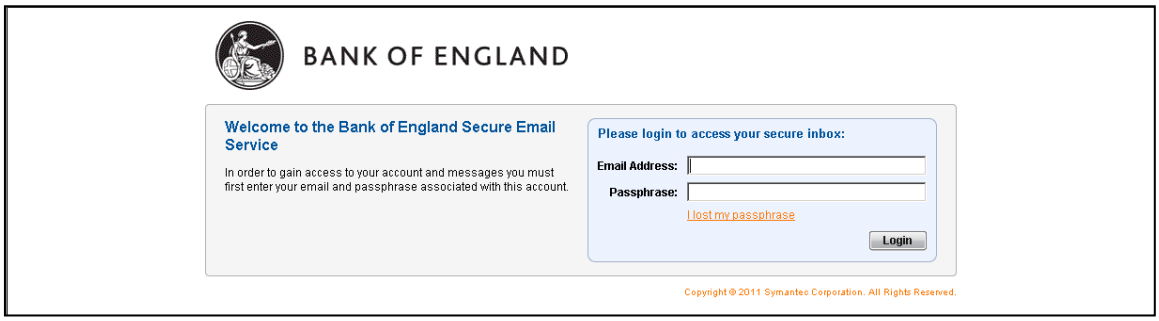
8 Web Messenger Account Administration

8.1 Changing Your Passphrase

- Go to https://keys.bankofengland.co.uk
- Enter your email address and your passphrase
- Select the **Settings** icon
- Select **Change my Passphrase** button
- You are prompted to enter and confirm your new passphrase
- Select the **Continue button** to register your new passphrase.

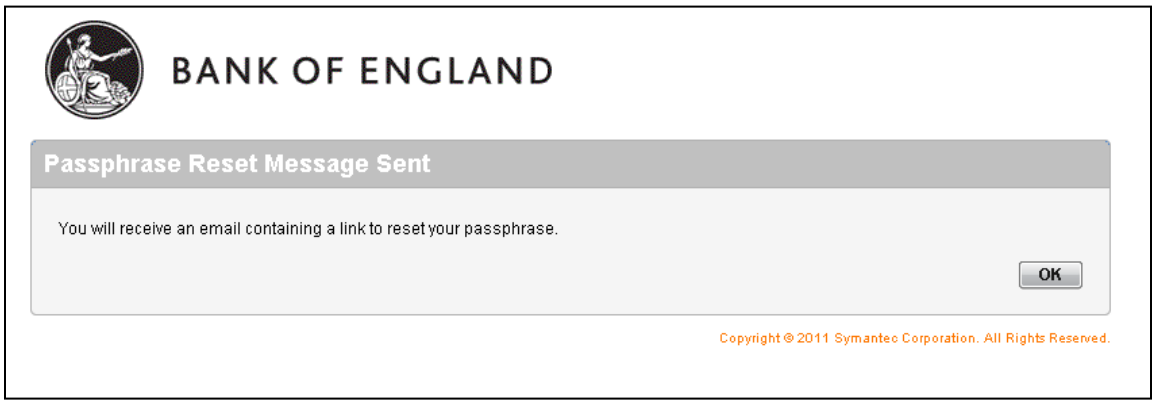
Note: The password expirations feature is disabled by default. The Bank of England user management policy ensures you create a strong passphrase by setting the 'Enforce minimum passphrase quality'.

8.2 Forgotten Passphrase – Resetting Own Passphrase



- Select **I lost my passphrase**

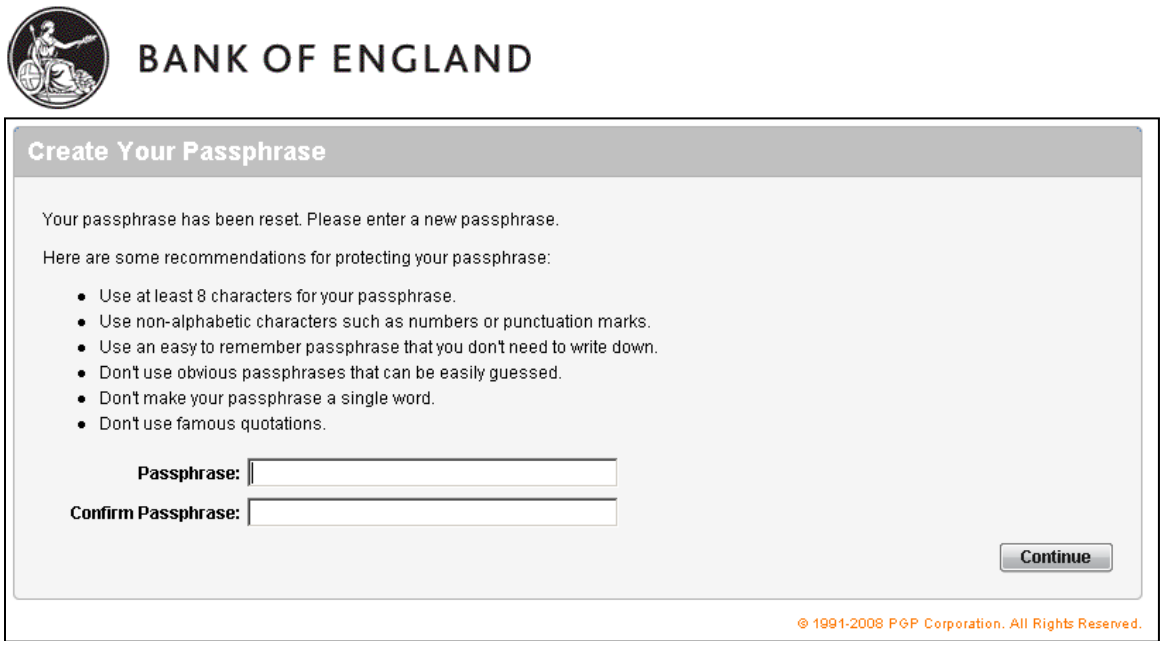
You will be asked to enter your e-mail address.



A message will be sent to your inbox with a passphrase link

- Select the link or copy and paste the link into your browser
- Create a new passphrase and confirm your new passphrase

Note: It is not possible to use the same passphrase as used before



Access to your mailbox is then permitted.

If you are still experiencing problems please contact your Bank contact

8.3 Account Deletions

We would be grateful if you could please inform us of personnel changes so we can remove old accounts from our PGP Web Messenger.

Accounts that have been inactive for **6** months will be automatically deleted with the removal of all emails

9 PGP Software

Select this option only if:

- You have a PGP Public Key,
- You currently use the PGP software for email encryption.

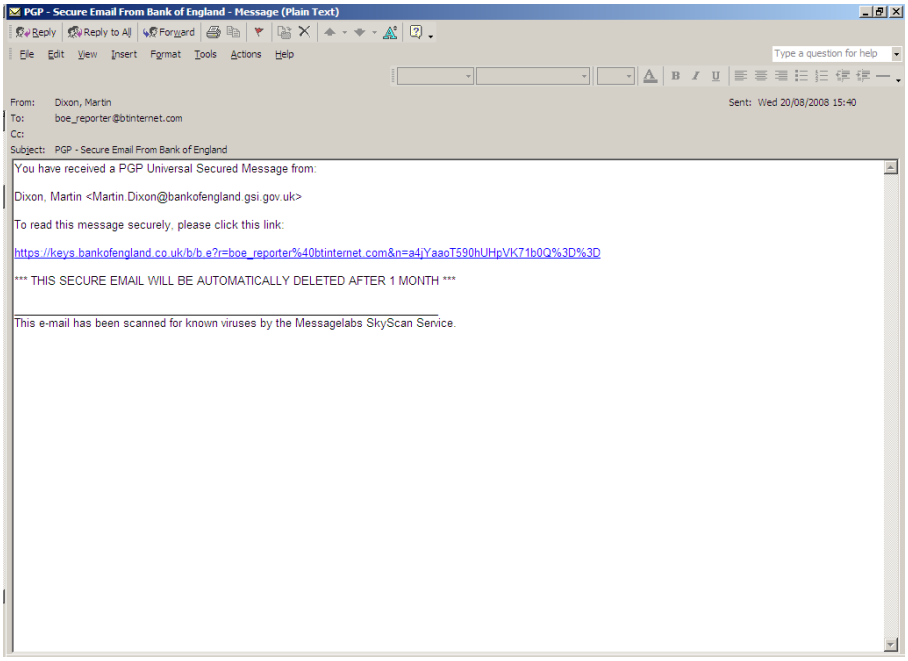
The Bank will try and automatically get access to your public keys, and if this is successful you will be able to continue to decrypt encrypted email received from your team.

If the Bank is unable to automatically get access to your public keys (due to organisations blocking access) then you will receive an enrolment email, which will ask you to upload your public key.

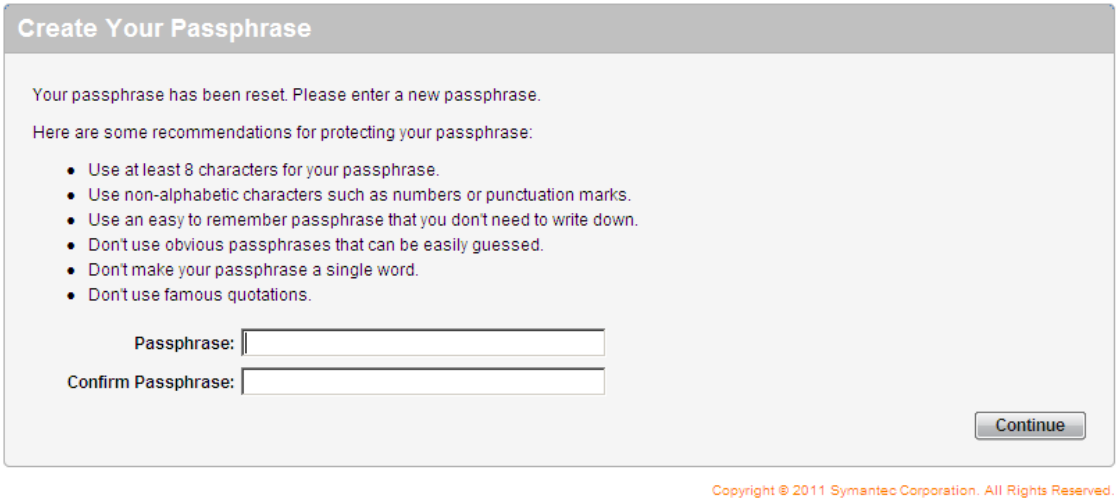
BANK OF ENGLAND

Instructions for uploading public key:

- On receiving an enrolment email from a Bank of England PGP user, you should **click on the web link in the message to create a passphrase** (see illustration below)



Click the link, and you will be prompted to create a passphrase (as illustrated below on the next page)



Enter your passphrase twice (in both the Passphrase and Confirm Passphrase fields) and select the **Continue** button.

You will see the Message Delivery Options window appear (as illustrated below)

- Select the **Key or Digital ID/Certificate** radio button
- Select **Choose Option**
- Follow the on screen prompts to upload your PGP key.

Alternatively we can email you the public keys you will require. If you would like these contact Data Reception (Tel. 020 7601 5360, *datareception@bankofengland.co.uk).*

10 Frequently Asked Questions

This is a selection of the most frequently asked questions along with answers. The contents will be updated on an on-going basis.

Does the introduction of PGP Web Messenger affect how I submit my statistical returns?

No, PGP Web Messenger does not affect how you submit your statistical returns and you should continue to use your current method (using BEERS or OSCA). Web Messenger will be used by the Statistical and Regulatory Data Division of the Bank to send you email communications relating to validation and cross form errors as well as plausibility questions.

We do not currently have PGP. Is this something we must acquire for Bank of England communications?

There is no need for any reporting institution to purchase or install any software or hardware to use PGP Web Messenger. However, if your institution has PGP, please contact us using the email addresses below.

Is there a software/licensing cost to use PGP Web Messenger?

There are no licensing costs for reporting institutions to use PGP Web Messenger.

Is enrolling on PGP Web Messenger a long process?

Once you have provided us with the email addresses/domain you use, the process of enrolling on PGP Web Messenger is a simple 2 or 3 minute process. The instructions for this are in the PGP user guide.

When are we required to enrol on PGP?

We began enrolling people onto PGP in November 2008 and a majority of reporting institutions now use PGP. However you can enrol at anytime.

I do not currently receive any/much email correspondence from SRDD. Does the introduction of PGP Web Messenger mean that I will start to receive (more) email correspondence from the Bank?

The introduction of secure email communication is not intended to alter the volume of communication the Bank has with reporting institutions.

Will emails I send to the Bank be protected?

Email communications sent from reporting institutions enrolled on Web Messenger to SRDD staff will be protected by PGP if you send the email via Web Messenger.

We have a similar product to PGP Web Messenger. Can I communicate with the Bank using this instead of PGP Web Messenger?

Some other products are compatible with PGP. To find out whether or not your product will work please contact Data Reception (Tel. 020 7601 5360, *datareception@bankofengland.co.uk).*

How do I send a message using PGP Web Messenger?

Click "Compose". In the "To:" text box, type in the email address of the person to whom you want to send a message. In the "Subject" text box, type in a subject for your message. Type your message into the text box under the subject. When you are finished, click "Send".

How do I delete a message?

Click the check box next to the message you want to delete. Click "Delete".

How do I read my messages?

From your "Inbox", click the message you want to read. When you are finished, click "Inbox" to return to the list of messages. To check for new messages, click "Inbox" again.

How do I attach a file to a message?

From a new email, click the paper clip symbol to attach the file. Find the file you wish to attach, double-click this and then select ok. The selected document should now be attached to the email.

How do I keep an audit trail of a message?

The body of the email can be saved locally from Internet Explorer, Click “File”, “Save as,” type “Web Page” and Click “Complete.”

How do I reset my passphrase?

If you have forgotten your passphrase please use the instructions found within our PGP user guide under the heading "Forgotten Passphrase".

BANK OF ENGLAND

How do I exchange PGP keys?

If your institution has recently installed PGP infrastructure and would like to swap PGP keys contact Data Reception (Tel. 020 7601 5360, *datareception@bankofengland.co.uk)* so that we can arrange to swap keys.

My email address has changed, what do I do?

If your email address has changed, we need to delete that PGP account and create a new one.

How do I check which email clients support PGP?

The latest version of PGP desktop supports the following email clients:

- Microsoft Outlook 2013 (32- and 64-bit)/Exchange Server 2010 (on-premise only)
- Microsoft Outlook 2013 (32- and 64-bit)/Office 365 Cloud Server
- Microsoft Outlook 2010 (32- and 64-bit)/Exchange Server 2010 (on-premise only)
- Microsoft Outlook 2010 (32- and 64-bit)/Office 365 Cloud Server
- Microsoft Outlook 2007 SP2 (Outlook 12)/Exchange Server 2007 SP2
- Microsoft Outlook 2007 SP2 (Outlook 12)/Office 365 Cloud Server
- Microsoft Outlook 2003 SP3/Exchange Server 2003 SP3
- Microsoft Windows Mail 6.0.600.16386
- Microsoft Outlook Express 6 SP1
- Microsoft Windows Live Mail
- Mozilla Thunderbird 3.0
- Lotus Notes/Domino Server 8.5.1 FP2
- Lotus Notes/Domino Server 8.5.2, 8.5.3

Mac OS X

- Apple Mail 5.x, 6.x
- Microsoft Outlook for Mac 2011

What is the difference between PGP and TLS?

TLS provides encrypted gateway to gateway delivery of all email between two organisations. Once the connection has been established, all email communication between the two organisations is secure. There is no need to set up individual users with

special software.

PGP enables end-point to end-point encryption and decryption of email sent over the Internet and requires each individual user to be set up with special encryption software.

How will I know whether my IT infrastructure is compatible with TLS?

TLS is compatible with all market leading mail servers including:

- Microsoft Exchange Server 2003;
- Microsoft Exchange Server 2007;
- Microsoft Exchange Server 2010;
- Sendmail 8.12
- Domino 6.5.

What are the Bank of England's cipher suite recommendations for TLS?

The Bank of England's TLS cipher suite recommendations are as follows:

- 256 bit encryption should be used.
- AES encryption cipher should be used.

The following ciphers should **not** be used:

- RC4;
- MD5;
- Anonymous Diffie-Hellman (ADH) suite; and
- SHA-2 certificate. (Please note that currently SHA-2 certificate mail sent over enforced TLS links to the Symantec Email Security cloud infrastructure will not be delivered.)

What is the Bank of England's Open SSL recommendation?

The Bank of England's Open SSL recommendation if used as part of your email infrastructure is as follows:

- OpenSSL 1.0.1g should be used.

- OpenSSL 1.0.1 – 1.0.1f should **not** be used.

What technical support will the Bank of England provide?

TLS and PGP — the Bank of England's Secure Email project team will provide you with support and advice during initial set-up. Once the solution has been enabled you will need to refer to your firm's IT support function to deal with any incidents or service

requests.

PDF Messenger — the project team will contact you with a step-by-step reference guide to guide you through the one-off registration process and how to send and receive email.

What does the Bank of England consider to be confidential information?

Examples of information considered to be confidential include, but are not limited to, the following:

• individual institutions returns to PRA & FSMA data;

• personal and staff information subject to the Data Protection Act;

• customer-related information;

• sensitive analysis and policy recommendations; or

• information given in confidence.

The compromise of this information could:

• materially damage the reputation of the Bank of England;

• damage the operational efficiency of the City, the economy, or financial markets;

• cause distress to individuals;

• breach proper undertakings to maintain the confidence of information provided by third parties (likely to include all customer data and individual institutions data);

• breach statutory restrictions on the disclosure of information including all personal information (staff, customer or other) subject to the Data Protection Act; or

• facilitate improper gain or advantage for individuals or companies, impede the investigation, or facilitate the commission of crime.

What if I do not want to receive secure email, or none of the options are suitable for my firm?

It is the Bank of England's policy to encrypt all confidential electronic communication, and the range of solutions offered are intended to meet the needs of the different types and sizes of firms. If your firm has a policy or any other reason why you cannot use one of the secure email solutions supported by the Bank of England, please contact the project team at prasecureemail@bankofengland.co.uk outlining why you believe this is not possible. Any exemptions to the Bank of England's policy go through a formal governance process and will be dealt with on a case-by-case basis.

If your question has not been answered above or you want more information on TLS, then contact Data Reception (Tel. 020 7601 5360, *datareception@bankofengland.co.uk).*