Secure Email

Frequently Asked Questions



Frequently Asked Questions

Contents

General Secure Email Questions and Answers Forced TLS Questions and Answers SecureMail Questions and Answers Glossary Support

General Questions and Answers

1. What is HSBC's security policy on email?

Security is a high priority for HSBC, especially when we are dealing with our customers and business partners' information.

It is HSBC's security policy to encrypt all emails that contain information which could pose a risk to our customers, business partners, clients or HSBC.

2. I already receive emails from HSBC which are encrypted by PGP. Will I still receive secure emails this way?

If there is already an agreement to use Pretty Good Protection (PGP) between HSBC and you then we can continue to use PGP to encrypt your emails. In future, we may migrate to only using Forced TLS and SecureMail however, you will be advised of this in advance. If you wish to have your messages encrypted by Forced TLS or SecureMail then please contact your HSBC Relationship Manager or HSBC representative.

3. I receive secure emails via another solution. Will I still receive messages this way? Yes, but in due course, we may migrate to only using Forced TLS and SecureMail when we need to send private or sensitive information to your personal or work email address. Exchanging messages by email is one method of communicating securely with you. You will still receive messages through your normal online banking or other existing secure communication channels.

4. What if my company uses a Third Party Processor for email?

If mail from HSBC goes via a Third Party processor which manages some or all aspects of your email service e.g. spam filtering or malware detection, then, if the mail has been encrypted by Forced TLS we can only guarantee it gets to the Third Party (as that is where our connection ends). You or your relevant company representative should speak with your Third Party email processor if you would like to keep the information secure between them and you.

There is no requirement for a Third Party email service company to be involved if the message has been sent encrypted by SecureMail as you only require your email account, Internet connection and access to a web browser to view your secure message.

5. My company has their own email encryption solution which must be used in accordance with the company's security policy. What do I do?

If it is HSBC that initiates the message then we will use Forced TLS if it is in place with you. TLS is fast becoming an industry standard and is now supported by the majority of mail server applications. Where Forced TLS is not in place with you, we will use SecureMail or an approved solution.

If you are intending to use your own email encryption solution to initiate or reply to messages then we request that you inform us of your solution in advance. Speak with your HSBC Relationship Manager or HSBC representative who will refer back to the relevant teams in HSBC. Please allow at least 7 days for HSBC to assess the solution and its use within HSBC. Your Relationship Manager or HSBC representative will confirm the result and next steps.

6. What if I do not want to receive secure encrypted emails?

HSBC takes information protection seriously and it is against our security policy to send information insecurely if it could pose a risk to you or HSBC should it be intercepted by an unauthorised recipient.

We will only send you a secure email if we are responding to a request or are required to send private or sensitive information which you prefer to receive by email. Speak with your HSBC Relationship Manager or HSBC representative to discuss other secure information transfer channels that suit you if you do not wish to receive secure encrypted emails.

Forced TLS Questions and Answers

7. What is Forced TLS?

Transport Layer Security (TLS) is a mail server feature which, once enabled encrypts the transmission of electronic mail from one organisation to another over the Internet. Forced TLS is a configurable TLS policy setting which ensures the email is only sent if the email can be transmitted securely.

8. Who is Forced TLS suitable for?

TLS is installed/ configured on email servers and therefore it is normally used by commercial/business organisations. TLS is fast becoming an industry standard and is now supported by the majority of mail server applications. HSBC has joined a growing number of organisations that have implemented it.

As TLS is an email server function it requires you or your company to be able to configure TLS on your mail server. If you are unable to do this then we will not be able to use TLS with you. For example, if you use a web based email service, you will not be able to manage these email servers.

If you use a Third Party to manage your emails then you may be able to speak with them about establishing a TLS link between you and HSBC.

9. Will using TLS cost me anything?

To send or receive emails securely via TLS, your email server must be configured to accept TLS email traffic. There may be a cost to you if either your current email infrastructure does not support TLS and new software needs to be purchased or you need to pay for IT work to configure your existing software. Once the appropriate work has been done the only ongoing cost will be for the yearly renewal of security certificates. You will not be charged per secure email that you send or receive.

10. Will I have to download or purchase any software to receive secure email via TLS? HSBC's preferred method of sending secure email is by Forced TLS which will work if Transport Layer Security (TLS) is enabled at both the sender and recipient's email servers. The correct server software is required to enable TLS and you or your company may need to purchase new software if, your current email infrastructure does not support TLS. If your company is using a Third Party to manage your email then establishing TLS connections may need to be negotiated with your Third Party.

If HSBC is unable to arrange a Forced TLS with you, we will not be able to send the email securely by TLS. In this case HSBC will choose an alternative approved solution to send the information securely.

11. How do I set up a Forced TLS connection with you?

Once you have confirmation that TLS is enabled on your email servers, please inform your HSBC Relationship Manager or HSBC Representative who will follow our internal process and make the necessary arrangements. This process can take several days to allow for our

IT team to complete implementation procedures and testing in conjunction with you or an IT representative from your company.

12. How will I view the secure message if it is encrypted by TLS?

If you receive an email encrypted by TLS, you will not need to take any specific action. The message will be delivered decrypted to your email inbox like any other email.

13. How do I know if TLS is working?

HSBC uses Forced TLS where possible to secure emails. Forced TLS guarantees the email will be encrypted by TLS and sent securely. This means if TLS is not working the email will not be sent. Please note this only applies to where Forced TLS is set up.

14. What if an email cannot be sent via TLS or TLS is broken?

Where Forced TLS is set up; whenever a TLS connection cannot be established with you the mail will not be sent and we will receive a Delivery Failure message. We will first retry over a period of time in case of any temporary TLS problems or, contact you to check whether you may be experiencing any TLS problems at your side. Further Technical assistance maybe required and we will consult with our IT support desk for further advice.

Where Forced TLS is **not** in place, the email will be encrypted by SecureMail or another approved solution.

SecureMail Questions and Answers

Receiving a SecureMail message
Replying to a SecureMail message
Forwarding a SecureMail message
Composing a SecureMail message
General SecureMail guestions and answers

Receiving a SecureMail message

15. I have received a SecureMail message but I can't find the message_zdm.htm' attachment referred to in my email. What do I do?

Depending on your mail reader, the attachment will be placed either to the top or bottom of the email. If you are still unable to find the attachment, please refer to the <u>Mail reader help</u> or contact your HSBC Relationship Manager or HSBC Representative that sent you the email.

16. How do I set up my SecureMail account?

You will be able to set up a SecureMail account when your HSBC Relationship Manager or HSBC representative sends you an email for the first time using SecureMail. If your organisation already uses the SecureMail solution provide by Voltage then you will not have to set up an account.

For a step by step guide to set up a SecureMail account, please see the SecureMail User Guide which is available at www.hsbc.com/secureemail.

17. How do I read a secure email sent via SecureMail?

To read your secure email, download and open the **message_zdm.html attachment**. On the page that opens in your web browser, click the **Sign in and Read Message button**.

If you already have an account, verify your email address and enter your password to sign into SecureMail. If you do not have an account, you can create one by following instructions on the screen or see the SecureMail User Guide available at www.hsbc.com/secureemail. After you are logged in, the secure message displays in your web browser.

18. How do I access attachments sent to me in my secure message?

Once you are logged in and your message is displayed, you can open any attachment by

clicking **View** or **Download** links next to the attachment name. If the programme is known, the attachment is opened automatically, if not, the attachment opens in a new browser window. You may also be presented with a pop up box giving you options to open or save the attachment to your own network drive.

19. What does it mean if the signature on my SecureMail message is marked valid with a ♥?

Every secure email is signed by the sender of the message to ensure authenticity of the sender and data integrity of the message. The means that the signature associated with this email is valid and the message can be trusted.

20. What does it mean if the signature on my SecureMail message is marked invalid with a \odot ?

Every secure email message is signed by the sender of the message to ensure authenticity of the sender and data integrity of the message. The means that the signature associated with this message is not valid and the message may have been forged. We recommend that you contact your Relationship Manager or HSBC Representative to check if the email is genuine.

21. Can I read my email encrypted by SecureMail on my Smartphone?

SecureMail messages are designed to be read from desktop or laptop computers only. Depending on your phone browser, you may still be able to access the message from your Smartphone however; this is not recommended or supported by HSBC.

Replying to a SecureMail message

22. How do I reply to a secure message on SecureMail?

You can reply to the message by:

- 1. Click **Reply** to reply to the sender or click **Reply to All** to reply to the sender and all copy parties.
- 2. This will take you to the reply screen. The senders email address is already entered in the **To**: field. If you click Reply to All, the copy parties will be included. You will not be able to add or remove any names in the **To**: or **CC**: fields.
- 3. Type your reply. The original message is already included in the composition area.
- 4. Click **Send Secure** to send your reply.

Please note that if you are sending a reply on behalf of your company; your normal company email disclaimer will not be shown in the reply unless you insert it manually.

23. How do I add an attachment to my reply message in SecureMail?

To add attachments to your reply:

- 1. Click **Choose File...** in the Attach field and select a file. The selected file is uploaded immediately.
- 2. To remove attachments, click **Remove**.

24. How do I get a copy of the reply that I have composed in SecureMail? By default, you will always receive a copy of your reply, click unless you click on the 'Do not send a copy to my inbox' option.

Forwarding a SecureMail message

25. Can I forward my secure message to other parties?

For security reasons, you will not be able to forward messages to HSBC or any other parties.

Composing messages in SecureMail

26. Can I use SecureMail whenever I want to communicate with you securely?

Yes, having received an email and registered for SecureMail, you can opt to compose a new message when signing out of the system. You can also bookmark the Sign In page for future use.

To compose a new secure message, log in via the 'Sign-In' page to create your new message. New emails can only be sent to HSBC representatives who are enabled to use SecureMail. Once the message is complete, click the 'Send Secure' button. A notification will be displayed once the secure message is sent successfully.

The compose new secure message window will be displayed where you can compose your message, add the recipient's e-mail addresses and a subject.

General SecureMail Questions and Answers

27. What is SecureMail?

SecureMail is an email encryption solution provided by Voltage Security Inc., and can be used with any email application. SecureMail is compatible with desktops, laptops and netbooks.

If you receive a secure message this way you will need to set up a SecureMail account. To set up the account and view your message, you will need connection to the Internet and access to a web browser.

28. How secure are SecureMail messages?

The secure email is encrypted with the equivalence of a 1024-bit key. It uses breakthrough Identity-Based Encryption to ensure the privacy of confidential information without compromising ease of use. Each message is also signed by the sender to ensure authenticity of the sender and data integrity of the message.

In addition, all decrypted email messages are viewed through your web browser using an SSL/TLS connection.

29. Is the SecureMail solution suitable for everyone?

Messages sent via SecureMail can be received securely by any email application. To view the secure message, you must also be connected the internet and have access to a web browser.

30. When I previously used Securemail, I downloaded an application for my BlackBerry. This application no longer works. Why?

Due to changing technology on BlackBerry and customer feedback, it was felt this application should be withdrawn. Depending on your phone browser, you may still be able to access the message from your BlackBerry. Customers can down load from the Apple, Android and RIM application stores to improve their experience when using a mobile device. However, viewing SecureMail messages on your BlackBerry and other Smartphones is not recommended and HSBC do not support these devices on our current infrastructure.

31. Will using SecureMail to read my message cost me anything?

There are no cost implications to receive or reply to emails encrypted by SecureMail.

32. Will I have to download or purchase any software to receive secure email via SecureMail?

There are no requirements to download or purchase any new software when using SecureMail.

33. I do not have TLS configured on my email server and do not have a web browser to view a SecureMail message. How will I be able to view the secure message?

If you cannot accept TLS email traffic and do not have a web browser to use SecureMail, we will not be able to send you the information securely by email using Forced TLS or SecureMail. Contact the originator of the message who can talk through appropriate solutions to sending the information via an alternative secure method.

Remember, it is against HSBC's policy to send information insecurely if the information could pose a risk to you, HSBC and other customers if intercepted by someone else.

34. How will I know the email has come from HSBC via SecureMail?

Every email that your recipient receives via SecureMail will contain the same anti-phishing image that is assigned to you on your first SecureMail email from your HSBC Relationship Manager or HSBC Representative. If you are ever in doubt please contact your HSBC Relationship Manager or HSBC representative by telephone rather than email.

35. Can my company set up one SecureMail account for all their employees? For security and technical reasons, each recipient of the email must have a SecureMail account to ensure the email is going to the authorised individual. Therefore your company cannot set up one SecureMail account for all employees.

If the email is sent to a shared email account, the owner of the account will need to set up a SecureMail account and share the account access details in accordance with your company security policies.

36. What about the possibility of SecureMail being blocked by Spam filters?

Spam filters work in different ways. They may filter emails by looking at the email header, subject line, email content or simply looking at the frequency the email is received from a source that you have not authorised. Depending on the spam filter used by your email service provider, email from HSBC encrypted by the SecureMail may be blocked or placed in your junk mail. If you are expecting an email but do not see it in your inbox, firstly check your junk box or if you have received notification that an email has been blocked, check the sender's email address. If you trust the source then you can continue to retrieve the email in the way that you normally do. You may also need to change the settings on your own filter - for example some settings prevent encrypted email being received.

37. Will all emails from HSBC be encrypted by SecureMail?

Emails will only be encrypted if the information contained could pose a risk to you or HSBC if intercepted by unauthorised recipients. If a Forced TLS connection is not in place with you, your email will be encrypted by SecureMail or an alternative approved solution that secures the information delivered to you.

38. I already receive email via Forced TLS. Will I now receive secure emails via SecureMail?

Forced TLS is HSBC's preferred email encryption solution. If we already have Forced TLS in place with you we will not encrypt the email by SecureMail.

39. Where can I find more information about SecureMail?

Visit www.hsbc.com/secureemail for more information about SecureMail.

40. Who can I contact for more help with SecureMail?

If you cannot find the answers you are looking for here or from any information provided on the www.hsbc.com/secureemail website, then please contact your HSBC Relationship Manager or HSBC Representative that sent you the email.

Glossary

Email Domain

Email Domain is the part that follows the @ sign in an email address E.g. name@youremaildomain.com

Email Server

An email server processes inbound emails in some way (e.g. filter spam) before it is delivered to the recipients email inbox.

Encryption

Encryption is the process of transforming data so it's unreadable to anyone except the party that is authorised to receive it.

Forced TLS - Transport Layer Security

Transport Layer Security (TLS) is a user transparent way of encrypting the transmission of electronic mail from one organisation to another over the Internet. TLS is a security protocol that is based on the Secure Sockets Layer (SSL) 3.0 protocol which has been in existence since 1996. Forced TLS is a configuration that has to be set on the sender and recipient's email server in order for the email to be transported securely.

Secure email

Secure email is an email that has been encrypted so that it can be sent securely over the internet.

Server

A server is computer system or device that manages network resources. Often servers act as storage devices for files.

SSL - Secure Socket Layer

Secure Socket Layer (SSL) provides enhanced security for internet communications. It uses **encryption** (see above) to ensure the confidentiality of sensitive information – such as credit card numbers, account balances and other financial and personal data – which is sent between a web browser and a web **server** (see above).

Web Browser

A **web browser** is a software application for retrieving, presenting, and traversing information resources on the World Wide Web.

Support

For further information about our email solutions, please refer to your HSBC Relationship Manager or HSBC representative. They will assist you or progress your query internally.

Issued by HSBC Holdings plc

We are a principal member of the HSBC Group, one of the world's largest banking and financial services organisations with around 8,000 offices in 87 countries and territories.

Published by Group Information Security Risk

8 Canada Square, London, United Kingdom E14 5HQ

© HSBC Holdings plc. 2013 All rights reserved.