

Transport Layer Security (TLS)

About TLS

Contents

Secure email at HSBC.....	2
About Transport Layer Security	2
Setting up a Forced TLS connection with HSBC	4
Glossary	5
Support	5

Secure email at HSBC

At HSBC we are committed to upholding the strictest security on information that we retain and how we can ensure that the information remains protected when we communicate with you. That's why we have made it our policy to encrypt and secure emails when they contain information that could pose a risk to you or HSBC if intercepted by someone else.

Wherever possible, HSBC emails which contain private and sensitive information will be sent from an HSBC email account using the security protocol called Transport Layer Security (TLS).

This secure email solution operates separately to our Internet Banking service.

About Transport Layer Security (TLS)

Transport Layer Security (TLS) secures emails transmitted over the internet using standard encryption technology. Securing emails this way reduces the risk of interception, eavesdropping and mail forgery.

TLS is now supported by the majority of mail server applications and HSBC has joined a growing number of organisations that have implemented it.

In addition to TLS, if you register your email domain details with us, we can implement a Forced TLS connection with you. Forced TLS ensures the email is only sent by us if a secure connection is negotiated with the client's mail server.

The following information provides more detail about how TLS works, who it's suitable for and how to set up a Forced TLS connection with us.

What is Transport Layer Security (TLS)?

Transport Layer Security (TLS) is an email security tool based on the Secure Sockets Layer (SSL) 3.0 protocol. It secures the transmission of email over the internet using standard encryption technology.

How does TLS work?

To work, TLS needs to be enabled on the mail servers of both the sender and the receiver of the email. Any information exchanged between the servers is encrypted, including the subject line, text and any attachments.

When sending encrypted messages, the mail exchange works as follows:

- When the sender connects to the recipient, the system automatically checks whether TLS is enabled on the client's mail server.
- If TLS is enabled at both ends, a secure TLS connection is established by using a 'handshake' procedure.
- During the handshake, TLS certificates are exchanged. If the sender's server trusts the certificate from the client mail server, the TLS session starts, and the email is sent via a secure internet connection.

Who is TLS used by?

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.

Why are organisations using TLS?

TLS has proved to be a stable and reliable service that requires no intervention by the email sender or receiver once it is available on both parties' mail servers. This means that both the sender and receiver can send and receive emails as they currently do today.

For these reasons TLS is fast becoming an industry standard which many financial institutions are planning to implement if they have not already done so.

What is Forced TLS?

Forced TLS is a configurable TLS policy setting which authenticates the destination email domain as a trusted source in addition to following the TLS process. This ensures the email is only sent if the email can be transmitted securely and the source is trusted. .

What are the other benefits of using TLS?

Greater Protection – Email servers can be configured to enforce TLS, (Forced TLS). This ensures that all emails are sent securely to a trusted party. At HSBC, our policy is to set up Forced TLS connections with customers, clients and third parties wherever possible.

Availability – TLS is available on most mail servers and is a globally accepted email security solution.

Allows emails to be scanned for viruses – Messages sent via TLS can still be scanned for viruses or malicious content just like regular emails.

Reduced costs – Where TLS is already a feature of the organisation's mail server, the organisation only needs to purchase the annual TLS certificate, unlike many peer to peer systems which require enterprise licences or licences per user.

Quick deployment – As TLS is configured direct with mail servers, the set up process is simple and does not require configuration for individual workstations. Time should be allowed for implementation and testing, which is a matter of days and not months. Once TLS is set up, emails can be exchanged as normal.

Setting up a Forced TLS connection with HSBC

As TLS is configured on the organisation's mail server, you should contact your technology department to find out if TLS is already enabled. If not, ask your technology department to activate TLS if possible.

Once TLS is configured, you can contact your HSBC Relationship Manager with the email domains that should be listed with us and contact details for your IT representative. Your HSBC Relationship Manager will forward these details to our IT department who will help with testing the Forced TLS connection with your IT representative.

We are also actively working with our customers, clients and third parties who have already used TLS with us previously to ensure we have all the information required to send emails via Forced TLS. You may choose to apply the same Forced TLS policy at your organisation. This will enable both parties to exchange emails securely at all times.

Glossary

Email domain

The email domain is the part after the @ in the email address. Your company may have more than one e.g. (e.g. hsbc.com, hsbc.com.hk)

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 that it is unreadable to anyone except the person that is authorised to receive it.

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

SSL – 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).

Support

Please refer to your HSBC Relationship Manager or HSBC representative who can progress your query to the relevant HSBC team.

Disclaimer

Transport Layer Security (TLS) is a security protocol that is based on the Secure Sockets Layer (SSL) 3.0 protocol. Messages sent over the Internet cannot be guaranteed to be completely secure as they are subject to possible interception, loss, or alteration. HSBC Holdings plc and/or HSBC Members (The Company) do not supply, maintain, support, license or otherwise derive a fee from a customer's use of TLS and therefore make no representations or warranties, including warranties of non infringement, performance, uninterrupted accessibility, delays, failures, errors, omissions, or loss of transmitted information. The Company is neither responsible nor liable for issues or damages incurred when using TLS to send and receive messages over the Internet.

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,
HSBC Holdings plc,
8 Canada Square, London, United Kingdom E14 5HQ

© HSBC Holdings plc 2011
All rights reserved