

Transport Layer Security (TLS)

Acerca de TLS

Contenido

Correo electrónico seguro en HSBC.....	2
Acerca de Transport Layer Security.....	2
Para establecer una conexión Forced TLS con HSBC.....	4
Glosario.....	5
Soporte.....	5

Correo electrónico seguro en HSBC

En HSBC tenemos el compromiso de mantener la seguridad sobre la información que guardamos y asegurarnos que la información se mantenga protegida cuando nos comunicamos con usted. Es por ello que hemos adoptado como política cifrar y asegurar los correos electrónicos que contienen información que pudiera representar un riesgo para usted o para HSBC si es interceptada por alguien más.

Siempre que sea posible, los correos de HSBC que contengan información privada o delicada serán enviados desde una cuenta de correo de HSBC con el protocolo de seguridad llamado Transport Layer Security (TLS).

Esta solución de correo seguro opera por separado de nuestro servicio de Banca por Internet.

Acerca de Transport Layer Security (TLS)

Transport Layer Security (TLS) se asegura que los correos se transmitan en internet con una tecnología de cifrado estándar. Asegurar de esta manera los correos reduce el riesgo de que sean interceptados, leídos por partes no autorizadas o falsificados.

TLS es soportado ahora por la mayoría de los servidores de correo y HSBC se ha unido al creciente número de organizaciones que lo han implementado.

Además de TLS, si registra la información de su dominio de correo con nosotros, podemos implementar una conexión Forced TLS con usted. Forced TLS se asegura que el correo sea enviado únicamente si se negocia una conexión segura con el servidor de correo del cliente.

La información siguiente da más detalles sobre cómo funciona TLS, quien puede usarlo y cómo establecer una conexión Forced TLS con nosotros.

¿Qué es Transport Layer Security (TLS)?

Transport Layer Security (TLS) es una herramienta de seguridad de correo electrónico basada en el protocolo Secure Sockets Layer (SSL) 3.0. Asegura la transmisión del correo en internet con tecnología de cifrado estándar.

¿Cómo funciona TLS?

Para que funcione, es necesario habilitar TLS en los servidores de correo tanto del remitente como del destinatario del mensaje. Cualquier información intercambiada entre los servidores está cifrada, lo que incluye el título puesto como asunto, el texto y los documentos adjuntos.

Cuando se envían mensajes cifrados, el intercambio de correo funciona como a continuación:

- Cuando el remitente se conecta con el destinatario, el sistema verifica automáticamente si está habilitado TLS en el servidor de correo del cliente.
- Si está habilitado TLS en ambos servidores, se establece una conexión TLS segura mediante un procedimiento de protocolo de intercambio conocido como "handshake" (apretón de manos).
- Durante este protocolo, se intercambian los certificados TLS. Si el servidor del remitente confía en el certificado del servidor de correo del cliente, inicia la sesión TLS y se envía el correo mediante una conexión de internet segura.

¿Quién utiliza TLS?

TLS se está convirtiendo rápidamente en una norma en la industria y es soportado ahora por la mayoría de aplicaciones de servidor de correo. HSBC se ha unido al creciente número de organizaciones que lo han implementado.

¿Por qué las organizaciones están usando TLS?

TLS ha probado ser un servicio estable y confiable que no requiere intervención del remitente ni del destinatario del mensaje una vez que está disponible en los servidores de correo de ambas partes. Esto significa que tanto el remitente como el destinatario pueden enviar y recibir correos electrónicos como lo hacen hoy día.

Por estas razones, TLS se está convirtiendo rápidamente en una norma de la industria, mismo que muchas instituciones financieras ya están planeando implementar, si no es que ya lo hicieron.

¿Qué es Forced TLS?

Forced TLS es una característica de política TLS configurable que autentica el dominio destino del correo como una fuente confiable además de seguir el proceso TLS. Esto asegura que el correo se envíe únicamente si se puede transmitir con seguridad y la fuente es de confianza. .

¿Cuáles son los demás beneficios de usar TLS?

Mayor protección – Se puede configurar los servidores de correo para que ejecuten TLS, (Forced TLS). Esto asegura que todos los correos se envíen con seguridad a una contraparte de confianza. En HSBC, nuestra política es establecer conexiones Forced TLS con clientes y terceros siempre que sea posible.

Disponibilidad – TLS está disponible en la mayoría de los servidores de correo y es una solución de seguridad de correo aceptada en todo el mundo.

Permite escanear los correos en busca de virus – Los mensajes enviados mediante TLS se pueden escanear para buscar virus o contenido malicioso al igual que con los correos normales.

Reducción de costos – Cuando TLS ya esté habilitado en el servidor de correo de la organización, ésta solo necesita adquirir el certificado anual de TLS, a diferencia de muchos sistemas inter pares (peer to peer) que requieren licencias corporativas o una licencia por cada usuario.

Rápida implementación – Como TLS se configura directamente en los servidores de correo, el proceso de alta es sencillo y no requiere configuración de estaciones de trabajo individuales. Llevará un tiempo implementar y hacer pruebas, pero será cuestión de días y no de meses. Una vez que se establece TLS, se pueden intercambiar correos como de costumbre.

Para establecer una conexión Forced TLS con HSBC

Como TLS se configura en el servidor de correo de la organización, deberá ponerse en contacto con su departamento de Tecnología para averiguar si ya está habilitado. De no ser así, pídale que, de ser posible, activen TLS.

Una vez que está configurado TLS, puede ponerse en contacto con su ejecutivo de cuenta HSBC para indicarle los dominios de correo que deberán aparecer en nuestra lista, así como la información de contacto de su representante de IT. Su ejecutivo de cuenta HSBC hará llegar esta información a nuestro departamento de IT, quien ayudará a su representante de IT con las pruebas de conexión Forced TLS.

Estamos trabajando también activamente con nuestros clientes y terceros que ya han utilizado antes TLS con nosotros para asegurarnos de tener toda la información requerida para enviar correos mediante Forced TLS. Puede escoger aplicar la misma política de Forced TLS en su organización, lo cual permitiría a ambas partes intercambiar correos con seguridad en todo momento.

Glosario

Dominio de correo electrónico

El dominio es la parte después de la @ en la dirección de correo electrónico. Su empresa puede tener más de uno (p. ej. hsbc.com, hsbc.com.hk)

Servidor de correo

Un servidor de correo procesa los mensajes entrantes de alguna manera (p. ej. filtro de correo no deseado) antes de enviarlos a la bandeja de entrada de los destinatarios.

Cifrado

El cifrado es el proceso de transformar los datos de manera que no los pueda leer nadie salvo la persona autorizada para recibirlos.

Correo electrónico seguro

Correo electrónico seguro es un correo que ha sido cifrado para que se pueda enviar con seguridad a través de internet.

Servidor

Un servidor es un sistema o dispositivo de cómputo que gestiona los recursos de red. Con frecuencia, los servidores actúan como dispositivos de almacenamiento para los archivos.

SSL – Secure Socket Layer

SSL proporciona una seguridad mejorada para las comunicaciones en internet. Utiliza el **cifrado** (vea definición anterior) para garantizar la confidencialidad de la información delicada –tal como números de tarjeta de crédito, saldos de cuenta y otros datos financieros y personales– que se envía entre el navegador y un **servidor** (vea definición anterior).

Soporte

Consulte con su ejecutivo de cuenta o representante HSBC quien puede canalizar su consulta con el equipo HSBC que corresponda.

Renuncia de responsabilidad (Disclaimer)

Transport Layer Security (TLS) es un protocolo de seguridad basado en el protocolo Secure Sockets Layer (SSL) 3.0. No se puede garantizar que los mensajes enviados por internet sean completamente seguros ya que están sujetos a posibles interceptaciones, pérdidas o alteraciones. HSBC Holdings plc y/o los Miembros de HSBC (la Empresa) no suministran, dan mantenimiento, soportan, otorgan licencia ni obtienen pago alguno por el uso que haga de TLS un cliente y, por ende, no otorga declaración ni garantía alguna, lo que incluye las garantías de no violación de derechos de terceros, desempeño, acceso ininterrumpido, demoras, errores, omisiones o pérdida de la información transmitida. La Empresa no es responsable ni acepta obligaciones por problemas o daños incurridos cuando se use TLS para enviar y recibir mensajes por internet.

Publicado por HSBC Holdings plc

Somos un miembro importante del Grupo HSBC, una de las organizaciones de servicios bancarios y financieros más grandes del mundo con cerca de 8,000 oficinas en 87 países y territorios.

Publicado por Riesgo de Seguridad de la Información del Grupo,
HSBC Holdings plc,
8 Canada Square, London, United Kingdom E14 5HQ

© HSBC Holdings plc 2011
Todos los derechos reservados