

Transport Layer Security (TLS)

Frequently Asked Questions

Data Classification: Nonsensitive

August 4, 2008



THE BANK OF NEW YORK MELLON



Table of Contents

Introduction	1
What is Transport Layer Security?	2
Why Use Transport Layer Security	4
Installing Transport Layer Security	6

Transport Layer Security (TLS)

Introduction

The Bank of New York Mellon actively works to protect the privacy and data integrity of sensitive client information while it is in our possession and control. In the course of providing services, we may exchange information with clients or their authorized representatives that is sensitive and confidential to the recipients. In order to protect this information when sending via e-mail, we will now encrypt e-mail communication by using a security protocol called Transport Layer Security (TLS).

TLS, an acronym for **Transport Layer Security**, is a feature of mail servers that encrypts the transmission of electronic mail from one server to another. Sending unencrypted messages increases the risk that messages can be intercepted or altered. TLS security technology is designed to protect confidentiality and data integrity by encrypting e-mail messages between servers and reduces this risk. TLS is a widely recognized standard issued by the Internet Engineering Task Force (IETF) for securing transmitted data and is now supported on most commercial mail servers.

This guide provides details about TLS: what it is, how it works, why it is important, and how you can install this security protocol on your organization's mail servers.

TLS is an IETF (Internet Engineering Task Force) standard for communicating e-mail securely. The Bank of New York Mellon did not develop the TLS technology. Nor does The Bank of New York Mellon or any of its affiliates supply, maintain, support, license or otherwise derive a fee from a customer's use of TLS. Accordingly, **THE BANK OF NEW YORK MELLON AND ITS AFFILIATES MAKE NO REPRESENTATIONS OR WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT OR FITNESS FOR A PARTICULAR PURPOSE, CONCERNING, AND HAS NO RESPONSIBILITY OR LIABILITY FOR, A CUSTOMER'S USE OF TLS, EVEN IF RECOMMENDED BY THE BANK.**

What is Transport Layer Security (TLS)?	
Question	Answer
<p>1. What is TLS?</p>	<p>TLS, an acronym for Transport Layer Security, is a feature of mail servers designed to secure the transmission of electronic mail from one server to another using encryption technology. TLS can reduce the risk of eavesdropping, tampering, and message forgery mail communications.</p> <p>TLS is a security protocol from the Internet Engineering Task Force (IETF) that is based on the Secure Sockets Layer (SSL) 3.0 protocol developed by Netscape.</p> <p>The TLS protocol is made up of two layers.</p> <ul style="list-style-type: none"> • The <i>TLS record protocol</i> is designed to protect confidentiality by using symmetric data encryption. • The <i>TLS handshake protocol</i> allows authentication between the server and client and the negotiation of an encryption algorithm and cryptographic keys before the application protocol transmits or receives any data.
<p>2. Is TLS something new?</p>	<p>TLS is the successor to Secure Sockets Layer (SSL). SSL and TLS are frameworks that include cryptographic protocols which are intended to provide secure communications on the Internet. TLS is the widely recognized standard issued by the Internet Engineering Task Force (IETF) for securing transmitted data. It is now supported on most commercial mail servers.</p>
<p>3. Who is using TLS?</p>	<p>The Bank of New York Mellon joins the growing number of financial institutions that have implemented TLS or will be doing so. The general consensus among financial institutions is that there is a need to protect the information that they exchange via e-mail from eavesdropping or tampering by third parties. Many financial institutions have already implemented TLS or they plan to convert to TLS by year-end.</p>
<p>4. How does TLS work?</p>	<p>When TLS is enabled on the mail servers of both the sender and the receiver of the e-mail, information exchanged between the servers is encrypted in a format that encodes plain text into non-readable form. Mail servers use Simple Mail Transfer Protocol (SMTP) to send and receive messages. When sending encrypted messages, the</p>

What is Transport Layer Security (TLS)?	
Question	Answer
	<p>mail exchange works as follows:</p> <ul style="list-style-type: none"> · Each company's e-mail gateway is configured to enable TLS communications for SMTP traffic · When the sending party (client) connects to the receiving party (server), the sending party checks whether TLS services are offered · If the receiver offers TLS services, the sender initiates a TLS handshake. The server sends its TLS certificate to the client · If the sender trusts the certificate of the receiver, a TLS session encryption key is negotiated, the TLS session starts, and the SMTP message is transmitted
5. Why is TLS so important?	<p>Sending unencrypted messages increases the risk that messages can be intercepted or altered. TLS security technology automatically encrypts e-mail messages between servers thereby reducing the risk of eavesdropping, interception, and alteration.</p>
6. What do I need to do to implement TLS on my e-mail server?	<p>Contact your internal technology support staff to find out if your organization has implemented support for TLS. If they have not, request that your technology staff implement TLS.</p> <p>Please reference the information regarding Installing TLS on the following pages to engage the TLS protocol.</p>
7. Do I need to contact the Bank after I implement TLS on my e-mail server to make it work?	<p>No. You do not need to coordinate your implementation with the company. After you have enabled TLS on your e-mail server, the server will automatically use TLS when exchanging messages with the company.</p>
8. What will happen if I do not want to implement TLS?	<p>Without TLS, you will still have the ability to receive and send e-mails with The Bank of New York Mellon. If your firm does not implement TLS, your e-mails exchanged with the company will not be secure, and will continue to use the unencrypted mail transport protocols that have been in use.</p> <p>There is risk associated with sending confidential information via e-mail through the Internet. If you choose not to secure or encrypt your e-mails to the company, The Bank of New York Mellon will not</p>

What is Transport Layer Security (TLS)?	
Question	Answer
	accept responsibility or liability for any unauthorized access to, or any loss, misuse or alteration of information exchanged between us.

Why Use Transport Layer Security (TLS)?	
Question	Answer
1. What are the benefits of using TLS?	<p>E-mail over TLS provides the following advantages compared to traditional (unencrypted) e-mail:</p> <ul style="list-style-type: none"> • Protection. E-mail servers can be configured to enforce TLS encryption between named parties and confidential information can be exchanged with reduced risk of eavesdropping or interception • Every e-mail sent and received is encrypted. When TLS is enforced, no individual review or decision is required to determine whether or not to encrypt an e-mail based on the e-mail's content. • E-mail encryption is transparent to both the sender and the receiver. Both parties send and read e-mails the same way as they do today. • TLS is globally accepted and currently available on most, if not all, e-mail servers. • Industry Standard. There is a growing trend among financial institutions to use TLS. These institutions have already implemented TLS or they plan to convert to TLS by year-end. • E-mail can be easily inspected for viruses. With SMTP over TLS, encryption terminates at partners' e-mail gateways. This means that after messages move inside a company's DMZ firewall, they can be treated just like regular SMTP traffic. Messages can be inspected, scanned and analyzed for malicious content to comply with corporate security policies. This is in sharp contrast to PGP- or S/MIME-style encryption schemes, in which messages are decrypted only at the point of

Why Use Transport Layer Security (TLS)?	
Question	Answer
	<p>receipt.</p> <ul style="list-style-type: none"> • Reduced cost. When company-to-company encryption over TLS is in place, tactical person-to-person systems for encrypting messages are no longer needed. In addition, companies need only purchase TLS certificates for servers, rather than large numbers of enterprise S/MIME certificates for all clients. There typically is no out-of-pocket cost to implement TLS, although there is some effort to set up and test TLS on the server, as there is no need to purchase any software. • No overhead for end-users. Because no special software is installed on client machines, TLS encryption is “always on” for compliant partners; the process is completely transparent to end-users. • Rapid deployment. Workstations do not require any additional configuration; only servers need to be modified. The configuration process is also straightforward. Time to value is measured in days and weeks, not months and years.

Installing Transport Layer Security (TLS)

What do I need to do to install TLS on my e-mail servers?

To implement TLS encryption for SMTP, you will need to:

1. Generate or renew a TLS certificate for your e-mail server (these certificates are similar to the SSL certificates used on web servers).
2. Install the TLS certificate on your e-mail server
3. Enable the TLS capability on the server
4. Send test e-mail to the bank and verify that the test was successful by examining e-mail headers

Note: it is generally advisable to implement and test TLS mail services on a test domain (or test host) first, *before* configuring production servers.

Step 1: Generate or Renew TLS/SSL Certificates

In order to encrypt e-mail traffic using TLS, the e-mail server must use a valid certificate. Certificates need to be generated or renewed on a recurring basis, depending on the validity period of the certificates. Most companies specify a validity period of one or two years.

The process for obtaining a TLS certificate for use with SMTP is identical to the one used to obtain a web server SSL certificate. Most companies are familiar with how to do this, and generally have their own preferred processes and solutions for doing so, using Open SSL or VeriSign for example. Instructions for using these solutions are straightforward and need not be repeated here. The steps that follow assume you have successfully generated public/private key pairs and obtained a new certificate from your firm's preferred Certificate Authority.

Note: Certificate renewal is extremely important to ensure that e-mail continues to flow normally. If your certificate expires, pending e-mails may be rejected by some domains. Your firm should have a process in place to ensure that you have sufficient advance warning of impending certificate expirations.

Contact your internal technology support staff to find out if your organization has implemented support for TLS. If they have not, request that your technology staff implement TLS.

Step 2: Install the certificate on your e-mail server

After you have created a TLS certificate, the e-mail server must be configured to use it for encryption, and for authentication with other domains. If you are operating a Microsoft SMTP server (such as the one provided with Exchange or the Windows server platform), the certificate can generally be imported from the Windows certificate registry into the SMTP server using a GUI interface. On UNIX- and Linux-based systems, the SMTP applications need to be configured to point to the location of the public/private keys and the certificate, generally from the command line or via a configuration file.

See the instructions for installing TLS certificates for specific SMTP server solutions in your product's documentation or online help material.

Step 3: Enable TLS policy on your e-mail server

Most TLS encryption services for SMTP servers can be configured to support different classes of e-mail service on an opportunistic or a per-domain basis. For example, policies can ensure that that for particular domains, your TLS-capable SMTP servers will:

- Always send/receive e-mails in plain text
- Use TLS if available, otherwise fall back to plain-text
- Always use TLS; if not available, refuse mail
- Always use TLS, and verify certificate CN match with the other party's fully-qualified domain name; otherwise, refuse mail

Not all servers support every option. You should refer to the appropriate documentation for your e-mail gateway software on configuring specific SMTP server solutions to enforce TLS policies.

Step 4: Test TLS over SMTP

Once the SMTP server has been configured, you can verify that TLS was used by examining the message header in a message from a domain that has enabled TLS, such as The Bank of New York Mellon. The "raw" message header should look similar to the following:

```
Received: from mail.example.edu (IDENT:smmsp@mail.example.edu [10.0.0.11]) by example.org
(8.12.1/8.12.1) with ESMTP id fBA0M7gU038106 (using TLSv1/SSLv3 with cipher EDH-RSA-DES-
CBC3-SHA (168 bits) verified FAIL) for <user@example.org>; Sun, 9 Dec 2001 16:22:10 -0800 (PST)
Received: from grue.example.edu (sender@grue.example.edu [10.0.0.13])
(authenticated bits=0) by mail.example.edu (8.12.1/8.12.1) with ESMTP id fBA0M3rD003797
(version=TLSv1/SSLv3 cipher=RC4-MD5 bits=128 verify=NOT) for <user@example.org>; Sun, 9 Dec
2001 16:22:07 -0800
```

```
Sender: sender@example.edu
Message-ID: <3C14002A.FAB442A3@example.edu>
Date: Sun, 09 Dec 2001 16:22:02 -0800
```

From: Sender <sender@example.edu>
To: user@example.org
Subject: test

References

A comprehensive reference for enabling SMTP over TLS for Postfix in particular:

<http://sial.org/talks/smtpauth-starttls/smtpauth-starttls>.

<http://postfix.state-of-mind.de/patrick.koetter/smtpauth>

Sendmail.org documentation:

<http://www.sendmail.org/~ca/email/starttls.html>

For the technical staff, the formal specification for SMTP is at:

<http://www.ietf.org/rfc/rfc2821.txt>

The formal specification for SMTP over TLS is at:

<http://www.ietf.org/rfc/rfc3207.txt>

You can also contact or direct other inquiries to your Relationship Manager or local Bank of New York Mellon representative.