TRANSPORT LAYER SECURITY FOR EXTERNAL PARTNERS

A guide to understanding how BNY Mellon protects the privacy and data integrity of sensitive information using TLS encryption of electronic mail.

May 2015

BNY MELLON | Invested

Introduction

TABLE OF CONTENTS

Introduction..... 2

Understanding TLS..... 3

Implementing TLS 5

Benefits Of Using TLS 7

Additional Information..... 8

TLS ENCRYPTION

BNY Mellon actively works to protect the privacy and data integrity of sensitive 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 which is sensitive and confidential.

In order to protect this information when sending such via electronic messaging, we encrypt email using the Transport Layer Security (TLS) protocol. Sending unencrypted messages increases the risk of messages being intercepted or altered. The TLS protocol is designed to protect confidentiality and data integrity by encrypting email messages between servers and reduces this risk.

TLS is a widely recognized industry standard issued by the Internet Engineering Task Force (IETF) for securing transmitted data and is now supported on most commercial electronic messaging infrastructures.

This document provides information regarding TLS, what it is, how it works, why it is important, and guidance to help you implement TLS in your organization.

Understanding TLS

WHAT? WHY? HOW?

- TLS is an acronym for Transport Layer Security.
- TLS is a security protocol used to encrypt email.
- TLS protects data and reduces risk of interception.
- TLS uses X.509 V3 digital certificates and asymmetric cryptography.

To use TLS encryption, our external partner organizations are required to have both a TLS capable infrastructure and a valid X.509 V3 public digital certificate for encryption issued by a trusted public certificate authority. No private certificates are permitted.

WHAT IS TLS?

TLS is an acronym for Transport Layer Security. It is a feature of electronic mail servers designed to secure the transmission of electronic messages between servers using encryption technology. TLS is a security protocol from the Internet Engineering Task Force (IETF) which is based on the Secure Sockets Layer (SSL) 3.0 protocol. The TLS protocol is made up of two layers.

- The TLS protocol is designed to protect confidentiality by using symmetric data encryption.
- The TLS handshake protocol which 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.

WHY IS TLS IMPORTANT?

Sending unencrypted messages increases the risk that messages can be intercepted or altered. TLS encryption technology automatically secures email messages between servers, thereby reducing the risk of eavesdropping, interception, and alteration.

HOW DOES TLS WORK?

When TLS is enabled on the mail servers of both the sender and the receiver of the email, information exchanged between the servers is encrypted in a format which encodes plain text into a non-readable form. Mail servers use Simple Mail Transfer Protocol (SMTP) to send and receive messages. When sending encrypted messages, the mail exchange works as follows:

- Each company's email 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. TLS (and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols which are designed to provide communication security over the Internet. They use digital certificates and asymmetric cryptography to verify the counterparty whom they are exchanging data with and to exchange a symmetric session key. This session key is then used to encrypt data flowing between the parties. This allows for data/message confidentiality, message authentication codes for message integrity and as a by-product, message authentication. An important property in this context is "forward secrecy," so the short term session key cannot be derived from the long term asymmetric secret key. As a consequence of using digital certificates, certificate authorities and a public key infrastructure (PKI) are necessary to verify the relation between a certificate and its owner, & generate, sign and confirm their validity.

TLS requires our external partner organizations to have both a TLS capable infrastructure and a valid X.509 V3 digital public certificate for encryption issued by a trusted public certificate authority prior to being able to send and receive encrypted email. Once established, this method is the most convenient for all users and provides seamless encryption for email and attachments. No private certificates are permitted.

Understanding TLS

NEW? WHO? TYPES.

- TLS first defined in 1999; based on previous technology.
- Widely used standard in the financial industry.
- The difference between ETLS & OTLS.
- TLS uses digital certificates for greater security.
- Certificate verification is a powerful tool to protect your secure connection from spoofing and invalid certificates. However, it also will interrupt mail flow if the recipient's certificate is not set up.

IS TLS NEW?

No. TLS is an IETF standards track protocol, first defined in 1999 and last updated in RFC 5246 (August 2008) and RFC 6176 (March 2011). It is based on the earlier SSL specifications (1994, 1995, 1996) developed by Netscape Communications for adding the HTTPS protocol to their Navigator web browser. TLS is the successor to Secure Sockets Layer (SSL). SSL and TLS are frameworks which 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.

WHO USES TLS?

The Bank of New York Mellon joins the growing number of financial institutions who have implemented TLS. The general consensus among financial institutions is that there is a need to protect the information exchanged in email from eavesdropping or tampering by third parties. Most financial institutions worldwide have already implemented TLS.

WHAT ARE THE TYPES OF TLS?

BNY Mellon requires TLS encryption of email containing sensitive and confidential information sent to and received from our business partners to protect the privacy and data integrity of data. While there are two types of TLS, the Bank of New York Mellon uses ETLS exclusively. All references of TLS in this document are, in fact, the enforced transport layer security (**ETLS**) type.

Enforced TLS (ETLS) forces TLS and prevents traffic if TLS is not established between the two endpoints of the connection. TLS is required at both the server side and client side. Some implementations allow finer control, like IP lists of servers to require TLS for. This feature provides customers who have strict compliance needs with a way to guarantee that messages to specific business partners on a per domain basis are always sent or received encrypted. Messages to and from enforced TLS domains which cannot be sent encrypted fail to be delivered to avoid exposure of the email content in plain text format on the internet. Customers can also use enforced TLS to ensure all email flowing between the customer and the service are transferred securely. ETLS requires valid X.509 V3 public digital certificates for encryption issued by a trusted public certificate authority, helping to make man-in-the-middle attacks less likely to succeed.

Opportunistic TLS (OTLS) means that a server will accept TLS connections from the client if the client asks for TLS in its handshake, but it won't require it. When the opportunity arises that a client does request TLS, a TLS session will be created and encrypt the traffic of the connection. This is useful typically for servers that don't always "know" to whom they're serving data to and must allow both TLS and non-TLS connections. If the administrator of the remote host has implemented TLS, regardless of whether or not the certificate used to facilitate the encryption is self-signed, the message content will be transferred encrypted. If the remote host has not implemented TLS, the service will still deliver the message but without the benefit of encryption. No configuration is necessary to enable this feature. The benefit of opportunistic TLS is that it works autonomously whenever possible to encrypt email, removing all ongoing management overhead. The downside of opportunistic TLS is that one party to the message has not implemented TLS, the email will still be delivered, but not encrypted.

Implementing TLS

PREREQUISITES & CERTIFICATES

- Establish a TLS partnership with The Bank of New York Mellon, fill out the Boundary Encryption Form to establish domain relationships. Contact The Bank of New York Mellon's TLS Administrator: tlsadmin@bnymellon.com.
- Purchase or renew a valid X.509 V3 digital public certificate from a trusted public certificate authority (these certificates are similar to the SSL certificates used on web servers). No private certificates are permitted.
- Install the valid X.509 V3 digital certificate on the appropriate mail gateway.

Ongoing certificate management is essential to maintaining continued successful protection of the privacy and data integrity of sensitive information.

BNY Mellon cannot answer questions regarding digital certificate costs.

PREREQUISITES

Already have TLS? Contact your internal technology support staff to find out if your organization has implemented support for TLS. If they have not, request they do so. Please reference the information regarding TLS in this section for an overview of the setup process.

Valid certificate? Your messaging technology resources must have a valid X.509 V3 digital public certificate from a trusted public certificate authority installed. These certificates are similar to the SSL certificates used on web servers. No private certificates are permitted.

Policy enabled? TLS policy must be enabled on your mail gateway server(s).

TLS partnership with BNY Mellon? In order to successfully use TLS encryption with BNY Mellon, you need to have your domain configured with BNY Mellon. To do this, request a Boundary Encryption Form and instructions from tlsadmin@bnymellon.com. Fill out the form and send it back to the TLS administrator at BNY Mellon at the same address. This form provides BNY Mellon with the technical information required to establish a link between your domain(s) and BNY Mellon's domains.

CERTIFICATES - INSTALLATION & MANAGEMENT

Purchase & Renewal. Digital certificates need to be purchased or renewed from a public Certificate Authority on a recurring basis, depending on the validity period of the certificates. Most Certificate Authorities specify a validity period of one or two years. The process for obtaining an TLS certificate for use with Simple Mail Transfer Protocol (SMTP) is identical to the one used to obtain a Web Server SSL certificate. Most organizations which have sufficient technology resources are able to implement digital certificates and generally have processes for doing so using Open SSL or VeriSign, for example.

Note BNY Mellon cannot answer questions regarding digital certificate costs. This is dependent on the selected public Certificate Authority.

Installation. After a valid X.509 V3 digital certificate has been purchased or renewed, the appropriate email gateway 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 (including the public/private keys) 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 must be configured to point to the location of the public key specified in the certificate. This is generally done from the command line or via a configuration file.

Installation section continued next page

Implementing TLS

ENABLE TLS & TEST EMAIL

- Enable TLS policy on the Mail Transfer Agent (MTA) servers.
- Test the TLS relationship.

It is optimal to implement and test TLS mail services on a test domain (or test host) first before configuring production servers.

Installation *(continued)*. Typically digital certificates are installed on the externally facing mail servers or gateways. The Public Key is what its name suggests - Public. It is made available to everyone in your digital certificate and via a publicly accessible repository or directory. On the other hand, your Private Key must remain confidential to you. You use your private key to encrypt plain text or to create your digital signature; whereas your recipient uses your public key to decrypt your encrypted text or to verify your digital signature. The term "asymmetric" stems from the use of different keys to perform these opposite functions, each the inverse of the other – as contrasted with earlier ("symmetric") cryptography which relies on one key to perform both functions.

Note Certificate renewal is extremely important to ensure email continues to flow normally. If your certificate expires, pending emails may be rejected by some domains. Your Certificate Authority should have a process in place to ensure sufficient advance warning of impending certificate expirations. Contact your internal technology support resources to find out if your organization has implemented support for TLS. If they have not, request TLS support to be implemented.

ENABLE TLS POLICY

The TLS policy [or policies] must be implemented, typically this is performed on the email gateway(s) or if the messaging infrastructure is hosted externally to your organization, then it is performed by your vendor.

TLS for SMTP is configured to provide encryption on a per domain name basis. Policies will ensure that, for particular domains, your TLS-capable SMTP servers will always use TLS and verify certificate Common Name (CN) matches with the other party's fully-qualified domain name. Otherwise email transmission will be refused.

This means, BNY Mellon must have your domain(s) configured. See TLS partnership with BNY Mellon.

Note You should refer to the appropriate documentation for your email gateway software on configuring specific SMTP server solutions to enforce TLS policies. BNY Mellon cannot provide technology support for our business partners' infrastructure.

TEST TLS OVER SMTP

Once TLS has been enabled, you can verify TLS was used by examining the message header in a message from a domain which has enabled TLS, such as BNY Mellon. The "raw" message header should look similar to the following:

```
Received: from xxxxxxxxx.bnymellon.com (xxx.xxx.xx.xxx) by
xxxxxxxxxx.xxxxxx.bnymellon.net (xxxx.xxx.xxx.xxx) with
Microsoft SMTP Server
id 14.3.123.3; Wed, 15 Jan 2014 11:40:01 -0500
Return-Path: <client @ domain name . com>
X-AuditID: xxxxxxxx-xxxxxxxxx-xxxxxxxxxx
Received: from mailxxx.xxxxxx.messagelabs.com
(mailxx.xxxxxxxxx.messagelabs.com
[xxx.xx.xxx.xxx]) (using TLS with cipher AES256-SHA (AES256-
SHA/256 bits))
```

Benefits Of Using TLS

ADVANTAGES OF USING TLS

- Data Protection.
- Automation.
- User Transparency.
- Industry Standard.
- Anti-Virus.
- Low Cost.
- Low Overhead.
- Rapid Deployment.

BENEFITS OVERVIEW

TLS has a number of benefits. First, it makes it more difficult for third parties to read email in transit. Second, when TLS is implemented with digital certificates issued by trusted certificate authorities, it can be used to establish the identity of the sending host. Additionally, TLS is transparent to end-users and easy to administer. Most importantly, using TLS allows BNY Mellon to further protect the privacy and data integrity of sensitive information while it is in our control.

ADVANTAGES

TLS provides the following advantages compared to traditional (unencrypted or “clear text”) email:

- **Data Protection**. Email servers can be configured to enforce TLS encryption between named parties and confidential information can be exchanged with reduced risk of eavesdropping or interception and can eliminate the risk of errors in transmission.
- **Automation**. Every email sent and received is encrypted. When TLS is enforced, no individual review or decision is required to determine whether or not to encrypt an email based on the content.
- **User Transparency**. Email encryption is transparent to both the sender and the receiver. Both parties send and read emails the same way as they do when unencrypted.
- **Industry Standard**. TLS is globally accepted and currently available on most, if not all, email servers. There is a wide spread use of TLS among financial institutions.
- **Anti-Virus**. Email can be easily inspected for viruses. With SMTP over TLS, encryption terminates at partners’ email gateways. This means after messages move inside a company’s 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 receipt.
- **Low Cost**. When company-to-company encryption over TLS is in place, tactical person-to-person systems for encrypting messages are no longer needed. Additionally, companies need only purchase TLS certificates for servers, rather than large numbers of enterprise S/MIME certificates for all clients. There typically is little 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.
- **Low Overhead**. Low overhead for administrators and none 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.

Additional Information

QUESTIONS

You can submit your questions in an email to tlsadmin@bnymellon.com.

You can also contact or direct other inquiries to your BNY Mellon Relationship Manager or local representative.

TLS & CERTIFICATE INFORMATION

References for the TLS protocol and digital certificates:

- http://www.ietf.org/rfc/rfc2246.txt
- http://en.wikipedia.org/wiki/X.509

SMTP OVER TLS FOR POSTFIX

References for enabling SMTP over TLS for Postfix:

- http://www.howtoforge.com/howto_postfix_smtp_auth_tls_howto
- http://www.postfix.org/start.html
- http://postfix.state-of-mind.de/patrick.koetter/smtpauth
- http://www.postfix.org/TLS_README.html#client_tls_encrypt

TECHNICAL SPECIFICATIONS

References for Sendmail.org documentation:

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

Reference for the formal specification for SMTP:

- http://www.ietf.org/rfc/rfc2821.txt

Reference for the formal specification for SMTP over TLS:

- http://www.ietf.org/rfc/rfc3207.txt

bnymellon.com

BNY Mellon is a global investments company dedicated to helping its clients manage and service their financial assets throughout the investment lifecycle. Whether providing financial services for institutions, corporations or individual investors, BNY Mellon delivers informed investment management and investment services in 35 countries and more than 100 markets. BNY Mellon can act as a single point of contact for clients looking to create, trade, hold, manage, service, distribute or restructure investments. BNY Mellon is the corporate brand of The Bank of New York Mellon Corporation (NYSE: BK). Additional information is available on www.bnymellon.com, or follow us on Twitter @BNYMellon.

05/2015

BNY MELLON | Invested