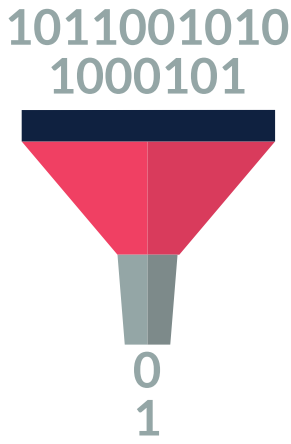


eFax Corporate® Transport Layer Security (TLS)

The eFax Corporate® TLS Service is a secure encryption solution that ensures the privacy and integrity of faxed documents while they are being transported via SMTP email over the Internet.

What is TLS?

TLS is the IETF (**Internet Engineering Task Force**) standard for "Transport Layer Security," and is the successor to SSL (Secure Sockets Layer) 3.0. TLS 1.0 was first specified in IEFT RFC (Request for Comments) 2244. The latest and most secure version is TLS 1.2 (RFC 5246), which is the version supported by eFax Corporate® TLS Service.

TLS is the encryption standard recommended by the National Institute for Standards and Technology (NIST) to protect sensitive communications. In addition, the Department of Health and Human Services (HSS) recognizes that the use of TLS is compliant with healthcare security regulations such as HIPAA. Furthermore, NIST has stated that SSL 3.0 should no longer be used due to a number of well-known security vulnerabilities.

The IETF also defines how TLS can be used to provide secure communications for SMTP email, namely through its RFC 3207, "SMTP Service Extension for Secure SMTP over TLS."

According to RFC 3207, SMTP over TLS:

"allows an SMTP server and client to use transport-layer security to provide private, authenticated communication over the Internet. This gives SMTP agents the ability to protect some or all of their communications from eavesdroppers and attackers."

How does it work?

The use of TLS is negotiated between SMTP servers by use of a single Service Extension to SMTP, known as STARTTLS. When the SMTP sender initiates the SMTP connection, it may issue this command to the SMTP receiving server to request that TLS is invoked on the same connection. If the request is accepted, the two servers will validate each other's certificates and the channel then becomes encrypted. After this point, all communications between the servers will be private.

Forced TLS

TLS has two modes of operation; opportunistic mode, and forced mode. The eFax Corporate TLS Service uses only the forced mode of TLS. With forced TLS, if the sending MTA is unable to establish a secure connection, the transmission will be terminated. In other words, all eFax Corporate® TLS fax transmissions must be encrypted, or the transmission will not take place.

Why use the TLS approach?

TLS has several advantages over S/MIME, another protocol for email encryption. First, certificate exchange and verification happens automatically within the protocol. There is no need to perform manual exchanges of certificates for every server with which you want to communicate.

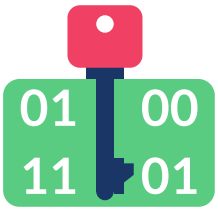
Second, S/MIME encrypts the message body, but not the message header information. Although the content might be encrypted, the subject, sender and recipient information are in the clear. By contrast, a TLS solution encrypts the entire channel, protecting the entire message, including any attachments.

Finally, as TLS SMTP works transparently between servers, it is unaffected by whether or not some messages have already been encrypted at the desktop by another method like S/MIME. This allows TLS to be combined with other encryption choices.

Standards

The eFax Corporate TLS Service is based upon the Internet standard for encrypting email communication, known as “SMTP over TLS” (or STARTTLS). STARTTLS allows the formation of an encrypted communication channel between a pair of mail servers, ensuring the privacy and integrity of any messages exchanged.

Subscribers using the eFax Corporate TLS Service will require a mail server (MTA) that supports STARTTLS. Fortunately, such support exists in the vast majority of commercial and non-commercial MTAs and so for most, no additional investment or technology deployment will be required.



Certificates and Authentication

The eFax Corporate TLS Service maintains two sets of certificates and accompanying private keys. One of these certificate/key pairs will be used when the service is acting in the role of the client — i.e., it is originating an SMTP session. The second certificate/key pair is used when the service is acting in the role of the server — i.e., it is accepting external SMTP communications.

Inbound Fax Authentication

Where the eFax Corporate TLS Service originates a TLS connection, the accepting MTA will need to provide its server certificate for authentication. If the accepting MTA wishes to authenticate the eFax Corporate TLS Service, then we will supply our client certificate for authentication.

Outbound Fax Authentication

Where an external MTA originates a TLS connection, then the eFax Corporate TLS Service will supply its server certificate for authentication, but will not normally insist on the external MTA supplying its client certificate for authentication. A subscriber may elect to have an authentication check made on inbound connections. eFax currently uses a VeriSign certificate for this authentication.

Certificate Validation

The validation of any certificate is based upon the identity of the Certificate Authority (CA) that has signed the certificate, together with a check on specific certificate content. For each certificate submitted by a remote mail server as part of a TLS connection, the eFax Corporate TLS Service will validate that a recognised CA has signed the certificate.

In addition, the certificate will be checked to ensure that it has not expired and that it relates correctly to the identity of the external mail server. If a certificate cannot be validated, then the connection will normally be aborted as it cannot be authenticated — and any associated messages will not be delivered.

All major CAs will be recognized by the eFax Corporate TLS Service. Self-signed certificates may also be used.

If you would like to learn more about outsourcing to a cloud fax model with eFax Corporate, visit us at ***enterprise.efax.com.au*** *or contact Sales at* ***1800 243 308****.*

About eFax Corporate

eFax® is the world's leading online fax solution, with more than 11 million customers worldwide. eFax lets users receive, review, edit, sign, send and store faxes by email or through a web interface. eFax offers plans for individual users and provides corporate solutions.

eFax is a brand of the j2 Cloud Connect division of j2 Global®, Inc. and a registered trademark of j2 Cloud Services™, Inc. and j2 Global Holdings Ltd.

To learn more about outsourcing to a cloud fax model with eFax Corporate, visit us at enterprise.efax.com.au

eFax Corporate®

Australian Headquarters
j2 Global, Inc.
Level 2, 39 Chandos Street
St Leonards NSW, 2065

Worldwide Headquarters
j2 Global , Inc.
6922 Hollywood Blvd.
Hollywood, CA 90028

Contact Sales:
1800 243 308

Web:
enterprise.efax.com.au

Please Recycle