U.S. FOOD & DRUG ADMINISTRATION

Welcome to Today's Webinar Setting up FDA Secure Email

Setting up FDA Secure Email

Presenter: Keith Robertson
Food and Drug Administration
Office of Information Management and Technology (OIMT)

Sponsored by the Center for Biologics Evaluation and Research (CBER)

Purpose

- The purpose of this Webinar is to provide information about setting up FDA Secure Email and become a Secure Email Partner

Scope

- For the purpose of this presentation, “FDA Secure Email” refers specifically to secure mail which is set up between the FDA and external entities.

Why do I need FDA Secure Email?

- Beginning October 1st, 2018, CBER-generated regulatory communications sent by email will only be sent to recipients via secure email.
- As part of the process of requesting a pre-assigned application number, you will be asked to set up FDA secure email. Additional information can be found on this website: https://www.fda.gov/Drugs/DevelopmentApprovalProcess/FormsSubmissionRequirements/ElectronicSubmissions/ucm114027.htm

Supported Options for Secure Email

- The FDA considers two methods as secure: S/MIME, and SMTP over TLS.
- In order to set up secure email with the FDA, one must have an email address or addresses set up with a unique domain name. Email provided as part of an ISP such as Comcast.net, Verizon.net, or AOL.com cannot be secured. Similarly, email addresses from one of the various free services such as Gmail.com, Yahoo.com, or ME.com cannot be secured.
- In order to request secure email, contact SecureEmail@fda.hhs.gov.

S/MIME Overview

- S/MIME secures a single email address at a time.
- S/MIME is more difficult to setup, use and maintain from the end-user standpoint, as everything is done on the workstation.
- S/MIME requires two things: a supported email client, and a digital certificate issued from a trusted CA (certificate authority.) SHA-256 certs are the current standard, however older SHA-1 certs that are not yet expired may be used.
- Examples of the most commonly used CA's by FDA S/MIME partners are: Globalsign, COMODO, and Symantec, although this list is not exhaustive.
- Self-signed certificates issued by oneself are not supported.

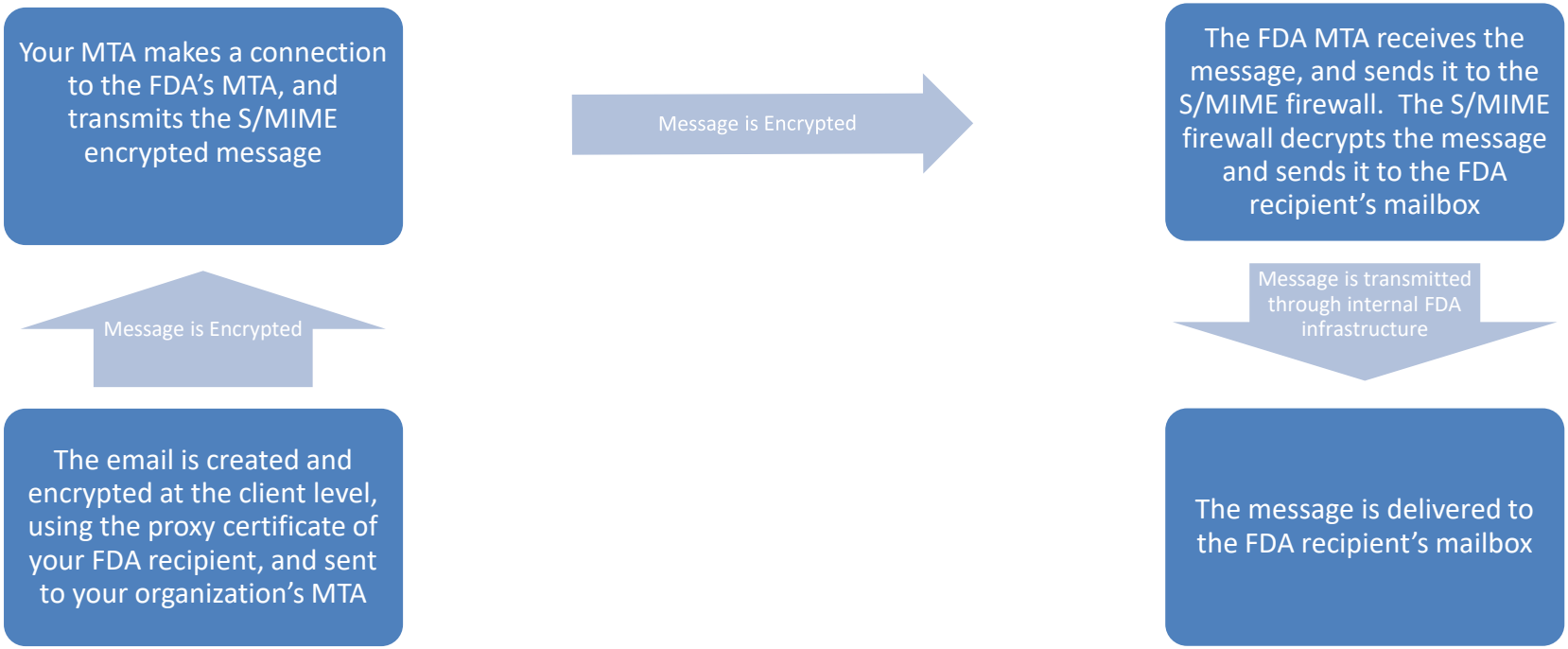
S/MIME (Continued)

- Digital certificates typically need to be renewed yearly or every three years. When a new certificate is installed on your workstation, it must also be provided to the FDA via an established process.
- Old certificates must also be retained on your workstation in order to decrypt and read older email.
- For each FDA address you want to securely communicate with, a one-time process is required to set up a FDA Outlook contact containing the corresponding FDA proxy certificate.
- In order to read S/MIME encrypted emails on a mobile device, your certificate will need to be installed on the device as well.

S/MIME Advantages

- Technically adept users can set this up themselves, without the need to involve their email administrators.
- “End to End” encryption can be achieved. The message is encrypted from your email client all the way to the FDA’s S/MIME firewall. Additionally, email sent to and received from the FDA remains encrypted in your inbox. Thus, even if your emails are stolen, they remain encrypted.
- Cost for a single user is around $60 for a one year digital certificate.
- After the certificate is installed, typical setup with knowledgeable IT staff is a couple of hours. After the first user is set up, the S/MIME instructions can be shared within your organization and users can be set up without intervention from the FDA Secure Email team.

S/MIME Message Flow



SMTP over TLS Overview

- Secure SMTP over TLS (RFC3207) is configured at the email server or host level, and only involves your email administrators. It will be their responsibility to ensure that all intermediate links between your infrastructure and the FDA and vice-versa are encrypted, and to perform all necessary testing.
- Once in place, SMTP over TLS will secure your entire domain. All email addresses ending in your domain name will be secured.
- For internally hosted email, a certificate will need to be purchased to secure the domain. A one year DigiCert SSL certificate is $175. A three year certificate is $420.

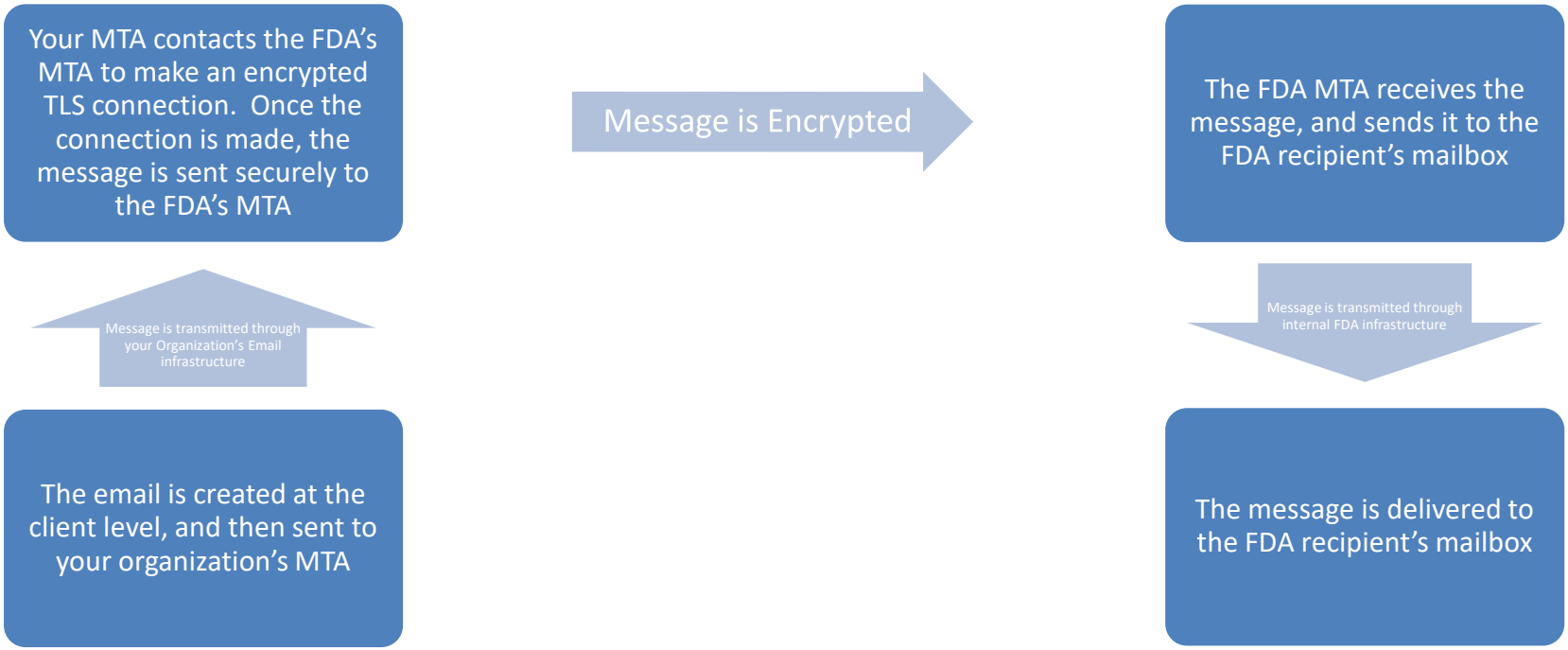
SMTP over TLS (Continued)

- For externally hosted (cloud) email, the necessary certificates are likely to be included as part of the service.
- If your organization's email system is internal, total setup time is likely to be one to two days for certificate purchase, provider verification and receipt, and then a couple of hours for certificate installation and a few emails between your admin and the FDA secure mail team for configuration and testing.
- If parts of or all of your organization's email system are externally hosted, the setup time may be longer as coordination with a third party could be involved.

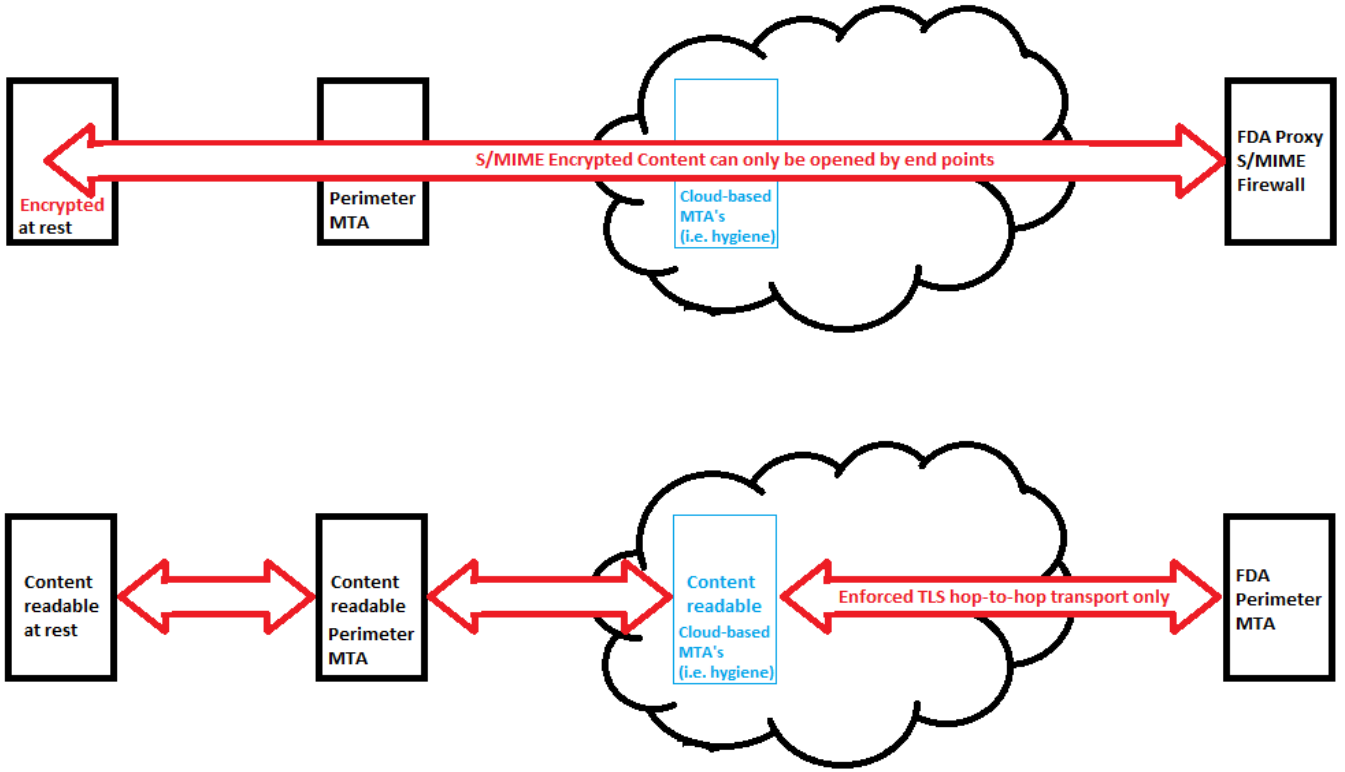
SMTP over TLS Advantages

- Once set up, your entire email domain is secured. Depending on how many individual user addresses will need to communicate securely with the FDA, this could result in considerable savings in monetary cost for certificate purchase, as well as setup time.
- No end user involvement is needed, as all of the changes are made at the server level. No special actions or configuration need to be made at the user level; email is sent as normal and the encryption is handled automatically between your organization's email infrastructure and the FDA's.

SMTP over TLS Message Flow



S/MIME vs. SMTP over TLS Comparison



S/MIME vs SMTP over TLS Comparison

- S/MIME is overall more difficult to maintain. However, it provides end to end encryption, from the sending client all the way to the FDA S/MIME firewall. The message can only be decrypted and read by these end points, and is persistently encrypted “at rest.” This means that if a message was stolen, it could not be decrypted.
- SMTP over TLS is simpler to set up, particularly for more than a handful of email addresses. However, care must be taken that each “hop” between MTA’s is set to TLS require, and the message is only encrypted in transit. The message is not encrypted “at rest” in the mailbox.

FDA Secure Mail Setup

- In order to request secure email with the FDA, send an email request to SecureEmail@fda.hhs.gov. This mailbox is monitored by the FDA Secure Mail team.
- A member of this team will review your request, and check to see if your domain is already configured for one of the two supported options.
- They will reply back to inform you that your domain has already been secured, or with an overview of the supported methods for your review. Once you have decided what method you would like to pursue, reply back and further instructions will be provided.

S/MIME Setup Highlights

- The FDA S/MIME solution has been tested with Outlook 2016 running on Windows 10, and Outlook 2016 running on Mac OSX 10.12.3 (Sierra) Instructions for these two clients will be provided. Older versions of Outlook and Windows have historically worked, however older versions of Outlook and Mac may not. For assistance setting up a client other than those which are FDA tested, please contact your local IT helpdesk.
- Once your digital certificate is installed, and if you are the first at your organization to set up S/MIME, email secureemail@fda.hhs.gov using the subject, “S/MIME Request.” The necessary routing changes will be made FDA-side.

S/MIME Setup Highlights (Continued)

- Once the FDA routing is in place, or if this has already been done, you can then set up your FDA secure contacts.
- To do so, send a digitally signed email to cert-query@fda.hhs.gov, with the subject being the email address of the FDA recipient you wish to securely communicate with.
- You will receive a reply containing the proxy certificate for that email address. From this reply, you must manually trust the FDA proxy certificate authority, and create a contact. You will use this contact to send securely to this specific address.
- The cert-query process must be completed for each FDA email address you want to send to securely.
- Additional S/MIME setup details will be sent during the request process from SecureEmail@fda.hhs.gov

SMTP over TLS Setup Highlights

- Your organization must set up “TLS Require” send connectors outbound to the FDA. Most MTA’s (Message Transfer Agents) will send with Opportunistic TLS by default. However, the FDA does not consider this to be secure as it opens the possibility of email being transmitted in clear text if the MTA’s are too busy, as well as “man in the middle” attacks.
- These TLS require send connectors will need to be set up to send not only to fda.gov and fda.hhs.gov, but also the legacy center-specific domains, such as cber.fda.gov.
- Additional technical setup details will be sent during the request process from SecureEmail@fda.hhs.gov

Frequently Asked Questions

- Q: “I sent a digitally signed email to cert-query@fda.hhs.gov, but a got a bounce-back. What did I do wrong?”
- A: Cert-query is only open to traffic from domains approved to utilize S/MIME. Send an email to SecureEmail@fda.hhs.gov, requesting that you would like to set up secure mail via S/MIME.

- Q: “I recently updated the digital certificate I use for S/MIME. What do I need to do?”
- A: Send a digitally signed email to cert-query@fda.hhs.gov. This will allow the FDA S/MIME firewall to capture your new certificate, and to begin using it for encryption and decryption.

Frequently Asked Questions

- Q: “I do not have a non-ISP or non-free email address, and I do not have an IT department to assist me. What is my easiest option?”
- A: There are a number of hosted email solutions, such as Office 365, Gmail for Business, or GoDaddy mail (among others) which can set up a unique email domain for you. Once set up, they should also be able to set up the TLS require option to secure your domain with the FDA. This carries the benefit of not needing any client-level configuration.

- Q: “I need to setup, or update my ESG account. Can you assist?”
- A: The FDA Secure Email team does not support ESG. Please try contacting their helpdesk at ESGHelpDesk@fda.hhs.gov. However, we can confirm that the same user-based certificate one would use for secure email via S/MIME can also be used for ESG. Please note that ESG and FDA secure mail are separate systems.

Frequently Asked Questions

- Q: “My company has a secure email solution in place, which sends an email with a link to the secure message. Does the FDA accept this as a secure solution?”
- A: At this point the FDA does not support this method of secure email. This method requires the recipient to click on an html link which redirects the recipient to an offsite mailbox. The FDA deals with hundreds of external partners all over the world. If the FDA permitted this type of secure email, then FDA personnel would have to maintain multiple passwords and logon accounts for external mail systems. Additionally, embedded html links in email is a prime spearphishing tactic for which there are few defenses. Thus, this type of secure email opens up the FDA to compromise.

Frequently Asked Questions

- Q: “I contacted my email administrators, who said that all of our emails are already sent using TLS. Can I proceed?”
- A: Most email systems will by default use “Opportunistic TLS” or “TLS Preferred.” The FDA only considers “TLS Required” to be secure, which will always force emails sent outbound from the FDA to be encrypted via TLS, and which will only accept incoming emails which were encrypted via TLS. Opportunistic TLS can in some instances allow email to be sent unencrypted. Please contact secureemail@fda.hhs.gov for the full SMTP over TLS instructions, which you may then send to your email administrators.

Webinar Questions

- Q: Please explain what a certificate is.
- A: A digital certificate is an electronic document used to identify an individual, server, company or domain, and provide recognized proof of the person or entity's identity. In relevance to S/MIME, the digital certificate will be used as proof of identity for an individual email address and provide digital signing and encryption for that address. In relevance to SMTP over TLS, the certificate will be used as proof of identity and provide encryption for an email domain.

Webinar Questions

- Q: When using SMTP over TLS, can secure emails be sent and received on mobile phones? Are there any special considerations similar to needing to install the certificate on the mobile phone when using S/MIME?
- A: Once SMTP over TLS is set up, the FDA secure mail team will verify that the connection from your company's MTA is being sent via TLS, and will guarantee that outbound email transmission from the FDA's MTA to yours is sent via TLS. Regarding mobile phones, this is something that your company's IT will need to address; that the connection from your mail servers to mobile devices is also encrypted.


FDA
U.S. FOOD & DRUG
ADMINISTRATION