National Institutes of Health

Office of the Senior Official for Privacy

Secure Email Services
PKI vs. SEFT

NIH staff often send emails containing personally identifiable information (PII) or other sensitive information. In an effort to ensure emails containing such information are properly safeguarded, NIH offers two *Secure Email* services: ***Public Key Infrastructure (PKI***) and ***Secure Email File Transfer (SEFT)***.

PKI is authentication software used to verify the identity of an email recipient through digital signature. SEFT is a web-based application that ensures the protection of PII and thoroughly secures all data and information being sent via email.

The purpose of this document is to provide a side-by-side comparison of PKI and SEFT and highlight the benefits and key features of both *Secure Email* services.

Public Key Infrastructure (PKI)	Secure Email File Transfer (SEFT)
Definition: **PKI** is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates. It is an arrangement that binds public keys with respective users identified by means of a certificate authority. The public key allows protection of the authenticity of a message by creating a digital signature using the private key, which can be verified using the public key. It also allows protection of the confidentiality and integrity of a message, by public key encryption, which can only be decrypted using the private key. **PKI** is recommended for smaller email communications.	**Definition:** **SEFT** is unique to NIH and was created as an alternative to PKI encryption. It is not a substitution for PKI, but it is the preferred platform to use when sending large attachments and documents. **SEFT** is a web-based *Center for Information Technology* service that allows NIH Users to send documents over a Secure Socket Layer (SSL) without having to obtain a PKI certificate. *Secure Email* extends the existing Secure File Transfer service to email messaging, enabling NIH Users to securely send and receive emails. While non-NIH customers cannot use *Secure Email* to ***send*** messages, they can **receive** encrypted email from the service. Using the *Secure Email File Transfer service* ensures the protection of personally identifiable information (PII) and thoroughly secures all data and information being sent via email.

Public Key Infrastructure (PKI)	Secure Email File Transfer (SEFT)
Please Note: *PKI secures the actual content.*	*Secure Email* also offers a level of non-repudiation and tracks correspondence history. Though PKI offers greater end to end protection, absent PKI capabilities, SEFT should be used whenever transferring sensitive, protected-health and/or PII information within the NIH community or external to the NIH Network. ***Please Note:*** *SEFT secures the transport of the content.*
Registration: For detailed instructions on obtaining PKI software, click on the following link: http://pki.nih.gov/PKI_request.htm	**Registration:** **Receiving:** All NIH employees and contractors are pre-registered to ***receive*** emails via SEFT. **Sending:** To receive permission to ***send*** emails via SEFT, NIH Users must contact the NIH Help Desk at: http://ithelpdesk.nih.gov/Support/ OR by calling: 301-496-4357 (local) 866-319-4357 (toll free) 301-496-8294 (TTY) OR By submitting a request using the web form found on the SEFT logon page at: https://secureemail.nih.gov/bds/Main.do
Obtaining PKI Certificates: The Department, through IAM@HHS Program, supports the issuance of two kinds of digital certificates to NIH staff: ***Smart Card Certificates –*** Are embedded in employees' NIH ID badges. However, there are specific configuration and user guides for different computer systems and/or software. Therefore, users should refer to the PKI User	**Logging Into SEFT:** Go to: https://secureemail.nih.gov/bds/Main.do 1. ***Enter Username***. NIH Users should only enter their NIH domain and login name (ex. Nih\doej). Non-NIH Users should use the email address to which they were first sent a *Secure Email*. Upon initial login this email address will become their

Public Key Infrastructure (PKI)	Secure Email File Transfer (SEFT)
Manual referenced below for details. ***Software Certificates –*** To obtain HHS PKI software certificates, NIH staff (including contractors) must: 1. Download the HHS Certificate Request Form at: http://pki.nih.gov/PKI_files/Certificate_Request_Form.pdf 2. Photocopy their NIH ID badge onto the Certificate Request Form, ensuring their picture is clear and recognizable. 3. Complete the *Applicant Information* section on the Certificate Request Form 4. Obtain their "Sponsor's" signature. (A government employee's Sponsor is a Federal employee in that individual's management chain (e.g., supervisor). The Federal Program Manager serves as the "Sponsor" for a Contractor. The AO, ISSO, or CIO may also serve as a Sponsor. After completing steps a-d above, Contractors and other non-Federal staff must: 5. Take the request form to their Local Registration Authority (LRA), which is a part of a public key infrastructure that maintains users' identities from which certification authorities can issue digital certificates. 6. Install the P12 file provided by their LRA on their computer. 7. If required, install the Common Policy root and/or HHS-SSP-CA intermediate certificates on their computer. 8. Configure Outlook and other applications on their computer to use the new digital certificates.	username. 2. ***Enter your password***. NIH Users will use their NIH login password. • If a user forgets their password, they can reset it by clicking the **'Forgot Your Password?'** link on the login page and follow the instructions. • If you are not a new user, you can request a password by clicking the **"New User – Request Your Password"** link on the logon page. ***Please Note:*** *For Non-NIH Users, your password must contain at least one upper-case letter, one lower-case letter, one number and one special character. NIH Users will use their NIH login password.*

Public Key Infrastructure (PKI)	Secure Email File Transfer (SEFT)
Sending Emails Using PKI Certificates: **To begin:** 1. Ensure that computer applications are configured to use the new digital certificates. (Detailed instructions are provided in the PKI User Manual). 2. Create an email message. 3. In the message, click the **DIGITALLY SIGN MESSAGE** button displayed as a little envelope with an award ribbon icon, located on the toolbar. 4. If the award ribbon icon is not displayed on your email toolbar, follow these steps: • Select TOOLS → CUSTOMIZE. • In the CUSTOMIZE window, click on the COMMANDS tab, under the CATEGORIES pane on the left. • Scroll down and click on STANDARD. • Under the COMMANDS pane on the right, scroll down to the DIGITALLY SIGN MESSAGE and ENCRYPT MESSAGE CONTENTS tool bar command buttons. • Select the DIGITALLY SIGN MESSAGE button. • Click **SEND.** 5. When the **ACTIVCLIENT LOGIN** dialog box appears, enter the **PIN** associated with the smart card and click **OK.** 6. After transmission, the email will appear in the recipient's inbox as a *digitally signed message*, indicated by the **DIGITALLY SIGN MESSAGE** icon. ***Please note:*** *After creating the email message, Smart Card users **must** insert their card into the reader (gold chip forward, facing up.) The ActivClient Login will appear requiring the user to enter their PIN number located on the*	**Sending Emails Using SEFT:** **To begin:** 1. Address your *Secure Email* the same as any other e-mail. 2. Complete the requisite fields. 3. Type your message. **4.** Consider assigning a password which adds an extra level of security (***Caveat***: ***The user must convey the password to the recipients through a medium other than the Secure Email (i.e. phone or other email).*** 5. Select **SEND.** 6. The recipient will receive an email notification containing a link directing them to either the login page (if the user is registered to ***send*** emails through SEFT) ***or*** registration page (if they are not registered to ***send*** emails through SEFT). ***Please note:*** ***NEVER*** *include sensitive, protected-health or personally identifiable information in the SEFT message notification box, as the box is not sent in a secure manner.*

Public Key Infrastructure (PKI)	Secure Email File Transfer (SEFT)
card. For users with Soft Certificates, if a password was created for the private key during certificate download, the user will be prompted to enter the password each time they send a signed email.	
Benefits: • PKI is an excellent way to send and receive encrypted email, allowing the user to login to computer systems with electronic credentials and digitally sign documents and e-mail. • PKI encrypts emails and verifies the recipient of the message. • PKI is utilized by a larger demographic, including both government and private sectors.	**Benefits:** • Provides NIH staff with a highly secure, "PKI-less" way to transfer files. • Provides users with the ability to send documents containing sensitive, protected-health and personally identifiable information securely. • Ensures the protection of confidential information. • Concerns relative to sender verification are eliminated, because a user must obtain permission to ***send*** emails via SEFT by contacting the NIH Help Desk. • Correspondence history is tracked.
Challenges: • Although PKI encryption methods work well for users who share a public key within one directory (like the Central Email Service at NIH), ensuring recipients outside that directory have access to the correct public key is not always practical. • PKI is not recommended for transmitting large documents.	**Challenges:** • Registration is required to ***send*** emails.
PKI User Manual: http://pki.nih.gov/PKI_PIVguides.htm#DIGSIG	**SEFT User Manual:** http://hr.od.nih.gov/hrguidance/issuances/infosecurity/documents/SEFTuserguide.pdf