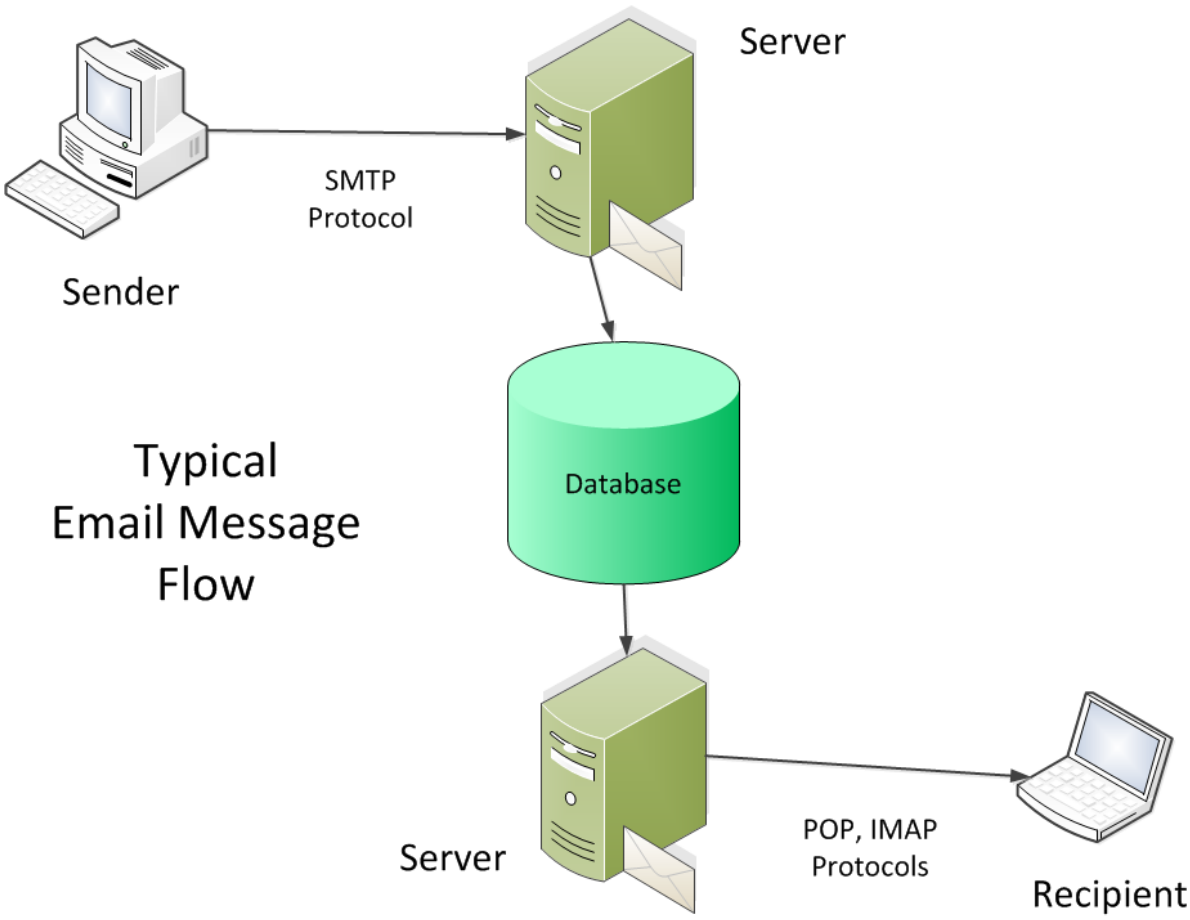
Private Email Security Overview

from

Secure Digital Communications

This document is intended for those who have already downloaded and installed a copy of the SDC Private Email to explain functionality unique to it needed to meet the requirements for security. Such functionality is absent in ordinary plain text (non-secure) email clients.

I. Operational Overview for Email Communications



Typically an email message originates from a person desiring to communicate with another over the Internet. The sender has his own email account with an address such as bobJ@email.com. The recipient would have his own account and email address such as fredF@differentemail.com. Both email users will have an application called an email client on their computer. There are more devices that can handle email but the PC and Laptop are the focus here.

A typical email client can originate and store the email that was sent as well as those received. Additionally such functions as Reply, Reply All, Forward, printing, adding and receiving attachments etc. are available.

The **SDC Private Email** (PEM) is no different except that all internal functions such as account setup and maintenance, contact setup and maintenance, encryption keys and the sent and received emails all have the relevant content encrypted by keys the user controls. There are

other email clients claiming secure content protection but many rely on external services such as public key rings, digital signatures, certificates, paid subscriptions to the email service provider who usually in one form or another has a say in **Key Management** (creation of keys, distribution and protection) etc.

The PEM differs completely from other email clients in those regards. The PEM does not rely on any third party 'trusted' services. Nor does the PEM require a subscription to a 'hardened secure server' service. The end users of PEM are the sole authority for the creation, distribution and protection of their **Session Keys** (SK). The PEM is capable of sending and receiving secure email messages utilizing popular public servers. The contents of those messages are not at risk even if the mail server database is compromised.

This sole responsibility on the user's part for **Key Management** will be a part of this document and a topic unfamiliar to most.

II. Security Starts at the 'Front Door'

Many email clients expose their full functionality to anyone who gains access to the computer including contact lists, copies of sent and received emails and attachments that were sent or received. PEM has a triple layer of encryption protection so that loss or theft of the hosting computer will not create a security threat if PEM and the computer are used correctly.

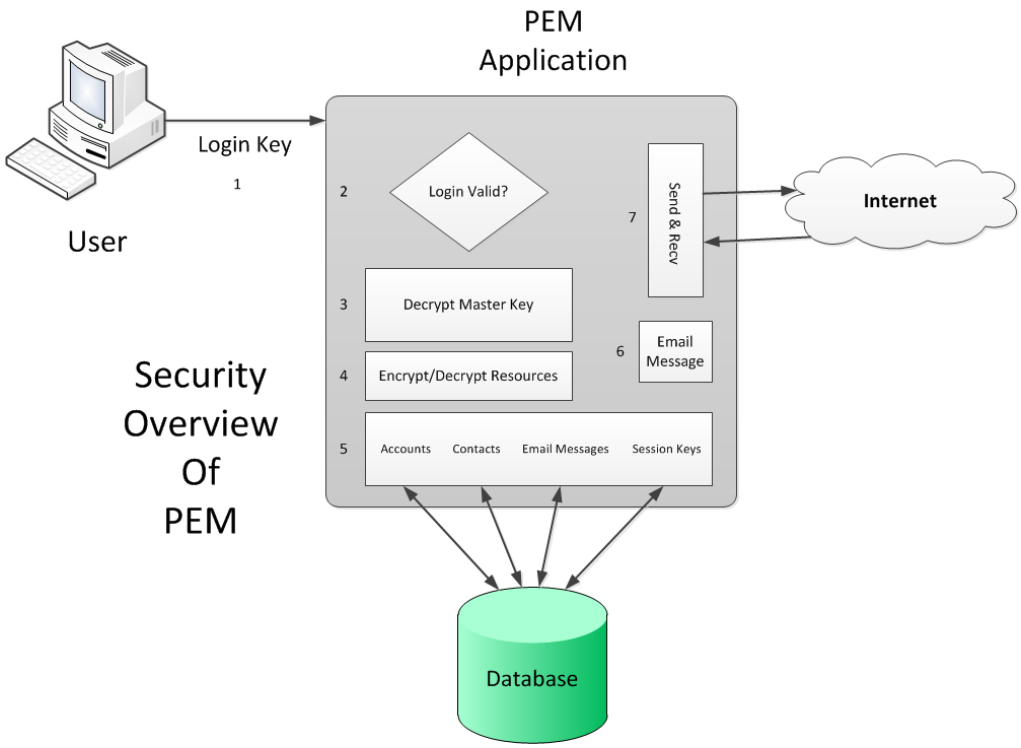


Figure 2. PEM Security Functionality

A. Typical User Workflow Security Measures:

1. Login (1 & 2)

The user inputs his Login Key which is a 256 bit AES encryption key. The submitted value if of correct form is hashed with SHA 256. This value is compared to the database value, if correct the Login process continues and the Master Key is decrypted with the Login Key. The Login Key value is discarded and startup continues with the Master Key.

2. Master Key Operations (3, 4 & 5)

The Master Key is used to decrypt needed resources for initial display. This includes the Account treeview control that selects the Account to view email from and the Account combobox that selects the Account to poll when **Retrieve Email** is clicked. There are no email messages or user Account, Contact or Session Key data that are not encrypted with the Master key. If some information or data is not visible on the screen then it is encrypted in the database. The Master Key is also a 256 bit AES encryption key. The Login Key and Master Key values may be updated independently of each other.

3. Email Message Operations (6 & 7)

Once Login is successful and startup is completed the user is able to view message content from the selected account. The selection of a particular Account **Inbox** or **Sent** folder causes information about the emails in that folder to be retrieved from the database and decrypted by the Master Key for display. When an email message is clicked on in the message listbox the contents are decrypted by the Master Key and displayed in the message view area. From this point the message may be **Printed**, **Replied** to, **Forwarded** or **Deleted** in the usual manner.

Polling for new messages is accomplished by selecting the Account to poll in the Account combobox then clicking **Retrieve Email**. Each email thus downloaded is first checked for correct form. It must be from a Contact using PEM or it is discarded. If the form is correct then the sender is authenticated as a valid Contact with an established **Key Relationship** or the message is discarded. If all is well at this point the **Session Key** shared by the user and the sender Contact is retrieved from the database and decrypted by the Master Key. The message is decrypted using the Session Key and then re-encrypted with the Master Key and stored in the database for use later.

Sending an email message begins in the usual manner. Click **New Message** and the lists of user Accounts and Contacts is retrieved and decrypted by the Master Key for use as the From and To parties. The user enters the Subject and message body text as is normally done. From here though, things change for security reasons.

When **Prepare To Send** is clicked multiple passes are made over the message body and meta data about the message is developed. This provides the means for the recipient to discover if tampering with the message has occurred enroute. Each recipient receives his message encrypted with his personal Session Key shared by the sender only.

When **Send** is clicked the prepared message and its embedded header is

encrypted with the recipient Contacts Session Key. If there is more than one recipient this process is repeated. Only one recipient per message is ever sent to the SMTP mail server.

4. Session Key Management (5)

To maintain secrecy of the Session Keys used between Contacts there must be secure protocols that the users agree upon and follow. All of the methods available to PEM users have stood the test of time and are in use today by governments, militaries, banks, corporations and others.

The first and most traditional is the physical exchange of key values by any desired means or combinations or means. The values thus exchanged may be encrypted by a **One Time Pad** for added security. The second and third methods available to PEM users both use the **Elliptic Curve Diffie-Hellman** (ECDH) key exchange protocol although in slightly different ways. The ECDH protocol allows to users to create a public-secret key pair (not to be confused with RSA) and exchange their public keys safely as they are useless to an adversary. Then the exchanged public keys are combined with the secret keys to produce the very same key value on both users computers. This key is also secret from the world and used only once and is known as a **Key Encryption Key** (KEK).

The Key Master in a Contact pair exchanging Session Keys enters or creates a new Session Key for the pair of them. The new Session Key is communicated to the Remote User Contact encrypted with the exclusive and mutually derived KEK.

If the Contact pair is exchanging keys for the very first time the **Distribute First Time Keys** functionality employing ECDH is used. The users exchange public keys and then the created or entered new Session Key is encrypted by the KEK and delivered to the Remote User via any means including ordinary email.

When the Contact pair already has a Key Relationship established the users may employ the **On The Fly Key Exchange** functionality in PEM. This method also utilizes ECDH the main difference being is the Key Master and Remote User have the option of using built in email messaging of the exchanged values encrypted with the current Session Key.

Support: stephen.tassio@topsecretcommunications.com