Overview

Electronic mail, commonly called email or e-mail, is used extensively in businesses as a means of communication. Businesses use email to send and receive information from colleagues and customers. The information in an email can be of a sensitive nature, therefore, it is important to ensure that the contents of sensitive emails are kept secret and to be certain as to the identity of the person who sent the email. Additionally, the email should be only viewable by the persons in the email address. Unfortunately, standard email on its own cannot ensure that the content of a sensitive email may be viewed or changed while in transmission. An email could be hijacked and viewed while the email is in transmission between two or more persons as the email is sent in clear text. There are many different mechanism that can be used to, for example, encrypt an email before it is sent, thereby ensuring that the email cannot be viewed if hijacked during its transmission between the persons involved. These mechanisms can be very complicated to implement and expensive to manage. One such mechanism is to use digital certificates to encrypt and digitally sign emails, but managing, training and supporting employees who use digital certificates can become too cumbersome and expensive for most businesses.

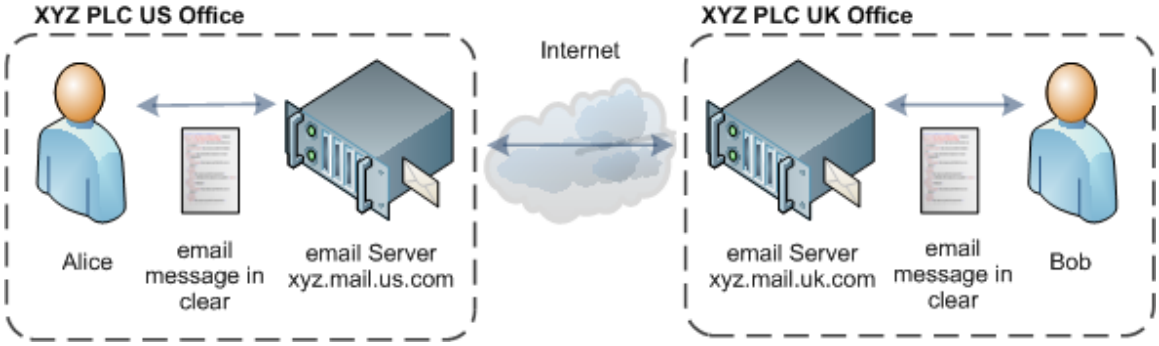
Versatile Security provides a product that solves this problem, the vSEC:MAIL® Server. The product sits in front of a companies email server and can be configured to digitally sign and encrypt emails before they are sent by employees. Using the vSEC:MAIL® Server removes the complexity for employees as they will continue to use their email clients as normal without the need to implement any new component in order to electronically sign or encrypt their emails.

How Does Email Communication Work?

In order to understand how the vSEC:MAIL® Server works it is important to understand, at a high level, how email communication works.

Suppose a fictional company XYZ PLC has two employees, Alice and Bob. Alice, a company lawyer located in the US communicates via email with Bob, who is also a company lawyer located in the UK. Often the email communication contains highly sensitive information that should only be viewable by Alice and Bob.

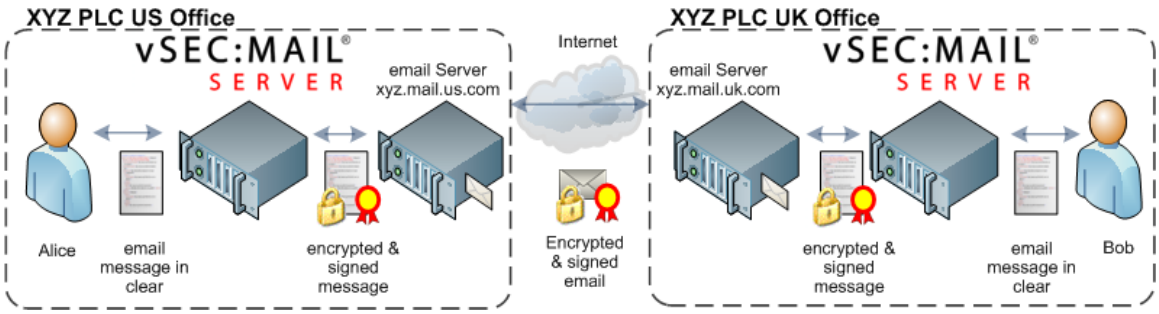
In a typical scenario, Alice composes a message using her email client, for example Microsoft® Outlook®. She enters the email address of her correspondent Bob, composes a message and hits the "send" button. Alice's email client then connects to her email server, *xyz.mail.us.com* and sends the email to Bob over the Internet. On its journey over the Internet, the email could easily be hijacked and the contents could be read and tampered with before Bob receives the email. Bob opens his email client to retrieve his email messages. His email client connects to his company's email server, xyz.mail.uk.com, and retrieves his email message from Alice.



The obvious problem here is that the email from Alice to Bob could be read and tampered with as it is transmitted over the Internet in the clear. This is unacceptable for the transmission of sensitive, confidential information via standard email.

How can vSEC:MAIL® Server Help?

The vSEC:MAIL® Server sits behind a companies email server and acts as a email secure proxy gateway. The vSEC:MAIL® Server can be configured to encrypt and digitally sign user emails before they are sent and correspondingly the emails will be unencrypted and the digital signature will be verified before they are received by the user.



The vSEC:MAIL® Server is simple to setup and configure by an administrator with the added advantage that the end user does not need to deploy any component in order to use the service. The encryption and digital signing of emails before they are sent, and the decryption and digital signature verification on receipt all happen transparently to the user. This will give the user the ability to send and receive emails in the knowledge that the emails are encrypted and digitally signed while in transmission. If an unscrupulous person intercepts an email that has been encrypted and digitally signed by the vSEC:MAIL® Server while in transmission they will not be able to read or change the contents of the email.