

# **PineApp™ Mail Encryption Solution™**

How to keep your outgoing messages fully secured.

**August 2009**

### **Modern day challenges in E-Mail Security**

Throughout the years, E-Mail has evolved significantly, emerging as a central means of communication.

The move to a computerized work environment has established e-mail as a legitimate and extremely widespread work aid, due to its obvious multiple advantages.

Unlike fax machine, for example, E-mail communication is instantaneous, especially during the last few years, with the wide spread of mobile handhelds supporting e-mail delivery.

E-mail based work is known to save multiple costs (and environmental friendly), in terms of saving paper, thanks to the major save in unnecessary paper printing. E-mail based work is also cost effective comparing to telephone based communication, sparing precious time and money wasted on long distance calls between organizations.

However, as any other technological innovation, once misused, E-mail based communication may carry some disadvantages and even dangers for one's organizational security, privacy & data confidentiality.

- A) Data theft** – Many business associates worldwide feel a false sense of security while sending emails containing classified and sensitive information insecurely during mail correspondence. Truth of the matter is, that just like telephone based communication, unsecured email correspondence can be “tapped”, and data can be easily retrieved by a malicious 3<sup>rd</sup> party. Opposing organizations and rival businesses can get their hands on precious information that shouldn't have been exposed to no one but the original sender and recipient, and target the retrieved information to harm your organization.
- B) Identity theft** – The SMTP protocol contains various security breaches, resulting in an insufferable ease of E-mail address forging (also referred to as “mail spoofing”). Spoofing is easily performed, even by using a personal computer's command line. The implications of mail spoofing on the business world are quite devastating: by forging one's mail address and pretending to be a business associate, one can retrieve confidential information quite easily. As a result, company's security is being compromised, and one's privacy is brutally invaded.
- C) Content compliance** – As a result of the SMTP protocol (and any other electronic mass means of communication) vulnerability and the sharp rise in content & identity theft cases, international security business regulations were amended, forcing almost all businesses worldwide to comply and force a strict data security policy in all realms. Examples for such rules are the GLBA & Sarbanes Oaxley regulations, forcing financial (and other) organizations to assume responsibility for enhanced security measures in any undisclosed data exchange (and also, undisclosed data storage).

### **Keeping it private – The usage of mail encryption**

Considering the above challenges, the importance of securing sensitive E-mail data is clear and crucial. The best way to keep your data secured and locked for anyone but the designated original e-mail recipient is by using E-mail encryption.

Mail content encryption, in its basic form, is performed using a pair of encryption keys (which are composed of a variable length random set of characters), exchanged by both parties, sender and recipient.

There are two types of encryption key pairs:

**Symmetric encryption key pairs** – a symmetric key pair is composed of two identical keys. In this case, the encryption key (sender) and the decryption key (recipient) are identical. Mail contents can be decrypted only by using an identical key & pre-configured password to the ones used for encryption.

**Asymmetric encryption key pairs** – an asymmetric key pair is composed of two keys, a public key and a private key, each contains a unique and different character set.

When using asymmetric keys, each correspondent holds 3 keys: 2 public keys (sender's and recipient's keys) and one private key.

At the beginning of a regular asymmetric mail encryption process, the sender requests the **recipient's** public encryption key. Once the recipient's public key is sent, the sender uses the **recipient's** public key to encrypt the mail content. The recipient uses his own private key (which is, of course, the only key that has the ability to perform decryption on mails encrypted using its paired public key), in addition to his pre-configured password, to decrypt the mail contents.

**Identity validation-** message encryption alone cannot fully guarantee mail content's security. As public keys may be located and replaced by a malicious 3<sup>rd</sup> party, once mail is sent via an unsecure route, sensitive mail contents can be decrypted and revealed by an undesignated, and probably hostile recipients.

Therefore, further security validation is necessary. Such security can be achieved by attaching to the encrypted mail message a special certificate, assuring sender's identity. Certificates are signed and given by a known certificate authority (CA) or a self signed certificate service, after a registration process that ensures and validates user's identity with full precision.

The sender attaches his own personal certificate to the encrypted mail message, thus ensuring that he indeed is the original mail sender.

### **End User to End User Mail Encryption – dangerous independence**

End to end encryption is performed, as its name may imply, by two end-users, using their desktop PC's. Both sender and recipient manage their own message content's security: they encrypt and decrypt their mails independently, usually by using special software or a mail client plug-in. They also manage and store their encryption keys and certificates independently, with no gateway or middle-device intermediation.

The consequences for such a work form may be problematic, and risky at some point, especially when both parties are business associates from peer organizations.

First of all, users are obligated to change their regular mail delivery behavior, by installing and using additional plug-ins and extra software.

Second, such a work form requires some technical knowledge, often unavailable at the simple end-user's level. Moreover, there are quite a few available encryption protocols (PGP, TLS etc.), many of which require full compatibility and supply partial or no support for other protocols' encryption. Therefore, end-users using specific incompatible software may encounter serious problems while trying to encrypt e-mails.

In addition, no content auditing, mail logging or inspection is performed by the end-user organization's IT department, as the mails are transferred via a secured route, separate from the route that all organizational mails are passing through. This way, sensitive data can be leaked out with no possibility of tracking.

Also, as mentioned above, public keys exchange is often performed using an unsecure route. Consequently, the original public keys can be captured and replaced by a malicious 3<sup>rd</sup> party, and sensitive mail content is exposed. Finally, there is the human cause: people often tend to forget and may encounter "button fatigue". As a result, when the encryption process is not automated, mails with sensitive information may be sent unencrypted and revealed to unwanted eyes quite easily.

Considering all of the above, one may easily understand the potential problems and risks in full reliance on end-user to end-user's approach in mail encryption.

### **PineApp™ Mail Encryption Solution™ – Introducing PineApp™ SES™**

PineApp have developed the Mail Encryption Solution, a new gateway based encryption module, integrated as a part of the award-winning Mail Secure product's policy engine.

This allows system administrator to gain full control, in terms of logging and content inspection, over outgoing mail encryption.

The detailed, yet intuitive and easy to use structure of the Mail-SeCure's policy engine enables an easy creation of various encryption triggers, on a base of a specific sender/recipient/domain, a specific file attachment(s) type and a keyword within a mail message. It is possible to have all mails coming out of the organization encrypted using an all inclusive policy rule.

IT managers who use the Mail Encryption Solution can design a fine tuned policy rule, like encrypting only outgoing mails with **PDF** files attached to them from the sender accounting@organization.com, due to the probably sensitive information they contain.

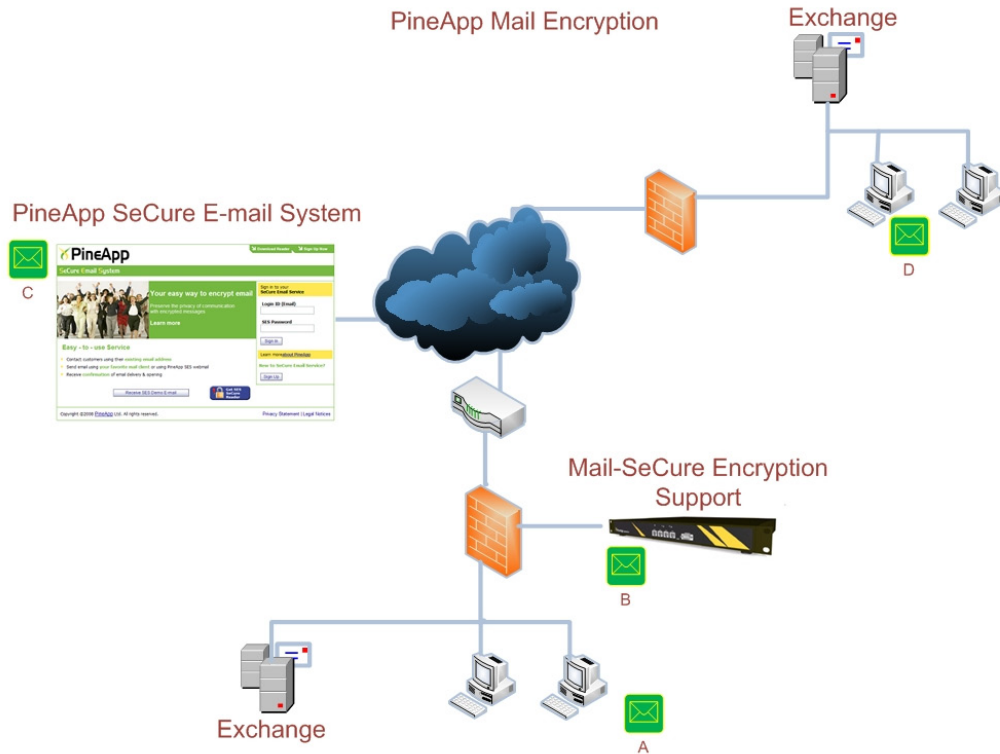
Encryption, however, is not performed on the appliance itself. Mails are forwarded in a secure route (SSL) to PineApp's On-Demand Secure Email System™ (**SES**).

PineApp SES is a designated encryption & certification center, automatically handling mail content's security for PineApp Mail SeCure clients worldwide.

Using a sophisticated set of rules and secured routes for both senders and recipients, PineApp SES assures your encrypted mail to arrive securely to its original destination(s) with no interruptions or risks.

**Encryption in action: The SES Registration method**

The PineApp Mail Encryption solution has an easy to use subscription – based system, making encrypted message delivery and reception easy and convenient, as shown in the illustration below:



- A)** Sender writes an e-mail message destined for encryption.
- B)** Organization exchange server forwards the e-mail to Mail-SeCure where it inspected for the presence of any encryption triggers. If such a trigger(s) is found, the email is moved to PineApp On-Demand SeCure E-mail System (SES) via secure copy connection.
- C)** The SES inspects and verifies that the recipient is registered. In case the recipient's mail address is registered, the mail message is immediately forwarded to the recipient's mail server. In any other case, the system parks the mail and sends a mail message, containing a notification about an encrypted message waiting for the recipient at the SES, and a direct link for the required service registration.
- D)** Encrypted message is sent only after the recipient registers and types the password he configured when opening the new encapsulated message.

**Mail Encryption solution Main Benefits –**

- The encryption solution is fully compliant with **Directive 95/46/EC, GLB, COX, HIPAA, PCI, Sarbanes-Oxley, BASEL II, HIPAA** and **GLBA** regulations.
- PineApp also offers In-LAN SES systems for enterprises and corporations.
- Multi protocol support (**S/MIME v2/v3, Open PGP, RFC 2440**)
- Possibility of working with other 3<sup>rd</sup> party vendors and encryption services, using the encrypted traffic forwarding feature.
- No learning curve or adjustment requirements from users, as they are required to no change in their original e-mail working habits in order to send encrypted mails.
- Full control, logging and content auditing available for system administrators, using PineApp Mail SeCure's intuitive log system.
- Flexible and uncomplicated policy engine, enabling easy determination and configuration of encryption triggers.
- No dependence on end-users and the "human cause", as encryption is controlled by the appliance according to organizational needs.
- Mails are fully secured until their opening – all encrypted mails are sent in a password protected PDF format
- Key/Certificate 'Burden' is handled by the PineApp SES and not by the organization.
- Reduction in IT costs, as the Mail Encryption Solution bundles with the Mail SeCure as an operable module, thus any need of an extra appliance for encryption only is spared, which also leaves you extra room for appliance in your rack mount.
- Saves bandwidth & processing power - the encryption process is being performed on PineApp SES, not on the appliance. That way, bandwidth and system resources consumption is reduced dramatically. Moreover, all keys and certificates are stored on the SES, thus an extra storage space is available, too!
- Mail Encryption Solution comes as a part of a full protection suite for your e-mail, along with the Mail SeCure multi layered defense.

### **About PineApp**

PineApp™, a leader in securing networks and email systems, offers comprehensive solutions for small, medium and large organizations.

PineApp's products are well known in the industry and have received very positive reviews, positioning them as leaders in their field.

Founded in 2002, PineApp is headquartered in Israel, with branch offices in the US, UK, Italy, Spain, France, Russia and South Africa.

In the past six years, PineApp has specialized in email and content security systems and already has significant presence in more than 50 countries. This specialty enabled PineApp to establish itself as a pioneer in developing unique and innovative engines to fight the different threats.