

# Simple Set-up

Two pieces of hardware are required to install the Secure-mail service, a hub and a USB stick. The USB stick is inserted into the back of the hub and information is uploaded. The hub will only accept information from a genuine Securecoms USB stick because we digitally sign the information and this cannot be faked.\*

During the installation process the hub randomly generates two unique email encryption keys – your private key and your public key. Your public key is used by others to encrypt the emails that they send you and your private key is the only key that can decrypt those emails. The hub holds your private key and the USB stick is overwritten with a backup of it – you must keep this safe. Unlike some other encryption services **we do not receive a copy of your private key**, which means that only your hub can decrypt the encrypted emails that are sent to you.

Once the installation is complete, your public key is sent to the Securecoms server where it will be logged in a database and shared with other hub users. At the same time, your hub will receive the database of other users' public keys. You do not need to manage keys. Key management is automatic and is one of the benefits of the Secure-mail service.

## Key facts

- Securecoms USB is digitally signed and secure
- Public keys are automatically distributed and maintained
- Private keys are known solely by the individual subscriber and not by us

## How it Works

The Secure-mail hub associates public keys with email addresses. Once installed, an email sent to a recipient using Secure-mail is automatically encrypted for its journey across the internet. When it reaches the recipient, their hub automatically decrypts the email. The encryption and decryption is performed locally by the hubs and not by a 3<sup>rd</sup> party which differs from some other services.

The sender and the recipient do not have to change the way they send or receive emails – there is nothing new to learn. If your recipient is not a Secure-mail user then the hub will not encrypt the email. (For encrypting emails between you and contacts without a hub please see below)

The hub is placed between your email server and your internet connection. It is a completely transparent bridge for all information except that which travels on port 25, the standard port for the email protocol SMTP.\*\*

Whenever your hub “sees” traffic on port 25 that contains your unique public key, it will automatically decrypt that email.

All other traffic passes through unnoticed and unaltered. No changes are necessary to any settings whether firewall, ISP, email server, email client, etc. It is completely plug and play.

Secure-mail uses the best possible encryption algorithms – AES (256 bit) and RSA (4096 bit). The email itself is encrypted rather than the communication stream, which differs from other services using TLS. These services can be vulnerable to “man-in-the-middle” attacks whereas Secure-mail is not.

The hub regularly receives software and key database updates from the Securecoms server. All updates are digitally signed and secure.

## Key facts

- Encryption and decryption is performed automatically
- No 3<sup>rd</sup> parties have access to your emails
- Email is composed, sent and received in the normal way
- No maintenance is required to the hub
- No configuration is needed

## Email Encryption for All

If you wish to send and receive encrypted email with contacts who do not have the hub service in place then you can offer them a free software version called **Secure-mail:lite**.

## Benefits of Secure-mail:lite:

- Easily offered to all your contacts – including the possibility of setting the hub to add a discrete message to your external emails, which contains a software download link.
- Software takes less than 3 minutes to download and install.
- Very simple to use.
- Microsoft Outlook users have a seamless plug-in.
- Capable of securely communicating with other hub users without any need for additional software (when invited to do so by other hub users)
- Ability for hub users to set up communities of Secure-mail:lite users when needed. Ideal when the hub user is working on a project with a number of external associates without hubs. The hub user can easily arrange for all parties to communicate securely with each other.

*\* Digital signing uses a mathematical process similar to asymmetric encryption. A piece of information can be signed using a private key. The public key associated with that private key can be used to authenticate the signature.*

*\*\* If in-house mail servers have been set up to retrieve email from an external mail server using RPOP then we can set the hub to examine traffic on the appropriate port.*