White Paper

Version 1.1

www.cyberens.eu

www.cyberens.fr

Introduction

The Simple Encryption Tool (SET) is a secure email client that encrypts/decrypts and anonymizes email end to end between a sender and multiple recipients. SET also provides the ability to categorize emails.

This white paper provides a technical description of SET's end-to-end encryption features. For a general description of the application, please visit www cyberens.eu/solutions.

The cryptographic primitives used in SET are both strong and fast. They are the same as in the TMS Cryptography Pack[1].

SET v3.0:

- allows users to exchange encrypted messages between each other using Windows PC;
- encrypts messages end-to-end for users having installed the application;
- does not replace a standard email application;
- generates and exchanges keys transparently;
- does not perform any statistics on what users do;
- does not send any other information in the background;
- does not need any other transport service or specific server to operate either than your email server;
- interacts with Cyberens' server to validate the license;
- retrieves authenticated updates.

This document provides an overview of the cryptographic services that are used in SET.

[1] http://www.tmssoftware.com/site/tmscrypto.asp

Terms

Asymmetric Key Types

- Identity Key Pair– A one year Curve 255-19 key pair, generated at installation time.

Symmetric Key Types

- Message Key– A 32-byte value.

Application Installation

At installation time, SET requests a few parameters:

- User name and password for SET
- Email account and password to send and receive messages (the password is required to query the email server)

Then SET generates the user key pair bound to the selected account, and sets its validity to one year (more accounts can be added later). The public part of the key is stored in a certificate containing a unique Id, a name, an email address and an expiration date. The certificate is then sent to Cyberens's server for signature (registered users only).

The user can send the certificate to any other user of SET. At no time does SET send the private key to a server but sends the certificate for each account to Cyberens' server for activation.

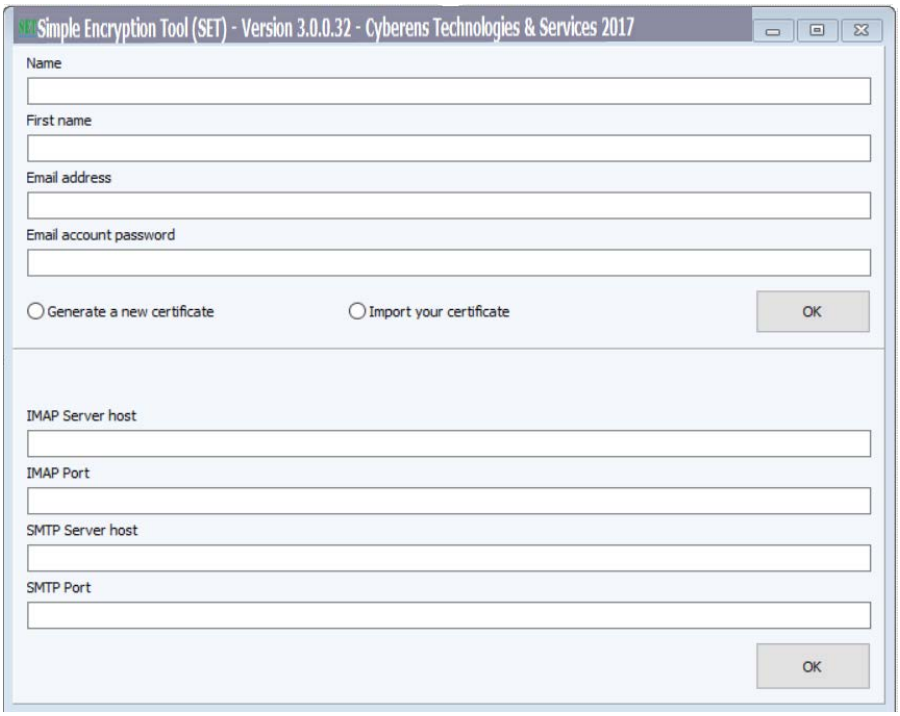

Figure 1: Installation View

Sending Messages

To communicate with another SET user, a user needs first to send her/his certificate to this other user. This is done by SET using a service email under the user's control.

Then to communicate securely:

1. The sender selects recipients in the contact list and types a message. Attachments can be added.
2. The sender then hits the "send" button.
3. SET generates a message key and "wraps" it with recipients' public keys.
4. The message body and the attachments are encrypted with the message key.
5. The message body is attached to the email with all attachments.
6. The resulting message is sent to all recipients with an anonymized title.

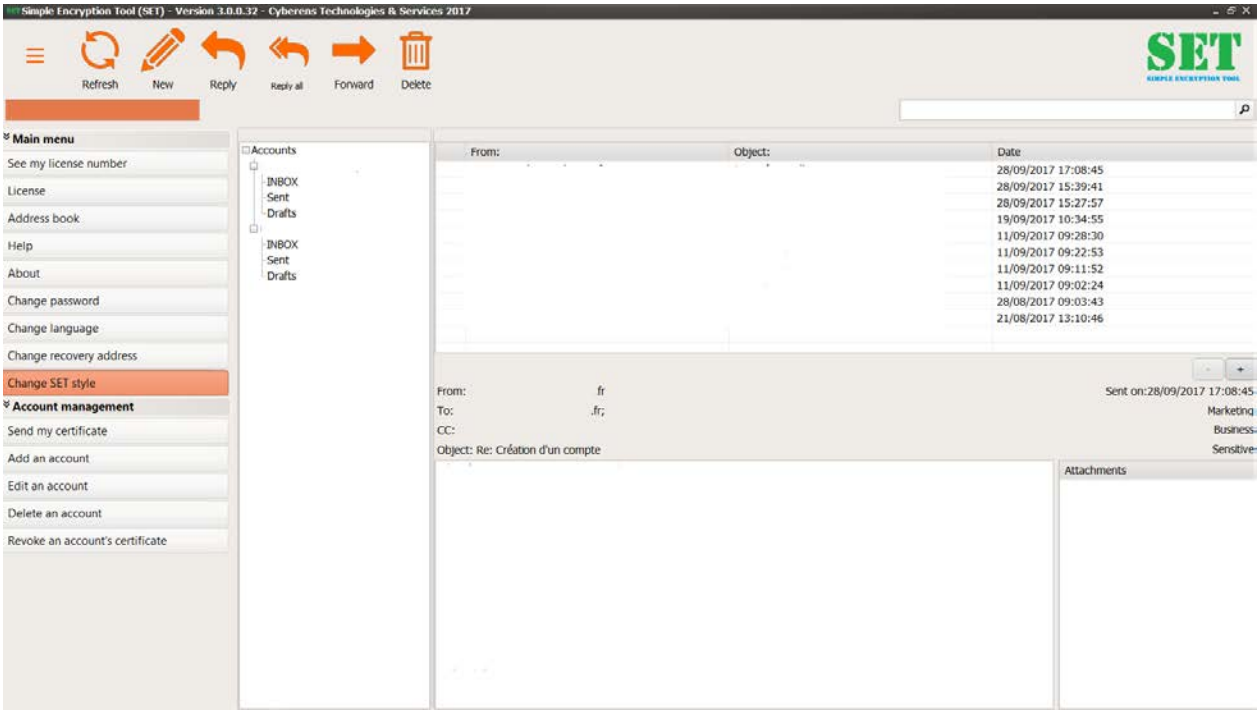

Figure 2: Main View

Receiving Messages

Several types of messages can be received by a user with SET: certificates and standard (encrypted) messages (SEM). All SET generated messages have a [SET_XX_DTG] object and are visible in any standard email client.

Certificates: are not displayed in any email thread.

Secret Keys: are encrypted and wrapped using ECIES and are not displayed in SET.

SEMs: are decrypted then displayed in a SET email thread.

Private Key Protection and Password Recovery

The private key is encrypted during storage with a secret key derived from the user password. While SET is in use, this private key is decrypted on the fly for each request (the password is stored in memory in a protected way).

It is however extremely important that the Windows PC is protected against malware and spyware that can target the password stored in memory.

SET has a password recovery mechanism. The key is encrypted locally with the server certificate and stored in a local security container. If a user loses the password, this container is sent (by the user) to the server that decrypts the password derived key with its private key and sends it back to the user in a protected way. The user can then unlock SET, change password and encrypt the private key again.

Getting Updates

Cyberens maintains SET and publishes regular updates to improve the applications. Each updates is signed with a specific certificate. SET is notified every time an update is posted on the server and asks the user whether it shall be installed (highly recommended). If the answer is positive, the update signature and integrity are verified, installed if the operations are successful, and SET is restarted.

Cryptography

SET uses the following algorithms and modes:

- The Advanced Encryption Standard (AES) with 256 bit keys in the Cipher Block Chaining (CBC) mode;
- The Password-Based Key Derivation Function version 2 (PBKDF2);
- The Secure Hash Algorithm version 2 (SHA2) with a 256 bit hash size;
- The Elliptic Curve Integrated Encryption Scheme (ECIES) with curve “255-19” with SHA-256 and AES-MAC-128.

The pseudo-random function is provided by the use of the Microsoft Cryptographic API for all cryptographic variables including initialization vectors. Each secret key is randomly generated and one time use.

Messages stored on the PC are encrypted with the AES (CBC) using a 256 bit key.

What is not addressed?

SET has been designed to protect messages using the SMTP protocol. There is no specific SET server either than the standard server set up by your ISP and the license management server used to activate the license. Consequently, recipient name, email address, time of sending, etc., are not encrypted by SET.

Conclusion

Messages between SET users are protected with end-to-end encryption that is deemed strong enough for sensitive but unclassified messages. Neither third parties nor Cyberens can read messages encrypted with SET. This can only be done by the sender and the recipient.