ELCRYPTO

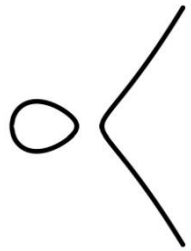
# Horizon

## User Manual

December 2014

ELLIPTIC CURVE CRYPTOGRAPHY TOOL FOR FILE ENCRYPTION

www.elcrypto.com



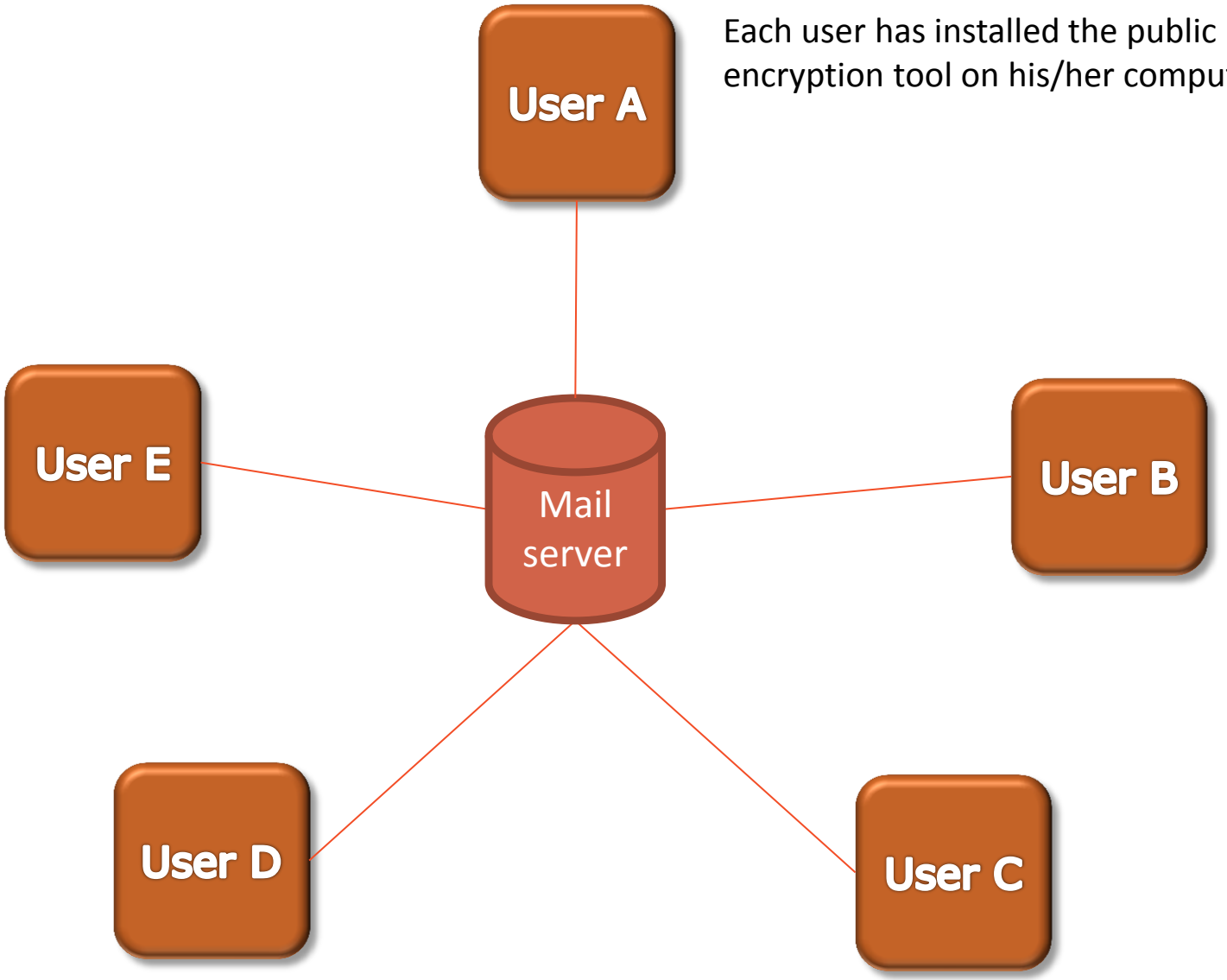
# Content


1. Introduction 3
2. Installation and System Requirements 8
3. Opening Screen 9
4. License Key 10
5. Entering My Username 11
6. Select an AES Security Level 12
7. Select a Type of Elliptic Curve 13
   - 7.a NIST Curves Setup 14
   - 7.b.1 Random Curves Setup 15
   - 7.b.2 Loading Parameters from External File 16
8. Loading Other Users' Public Keys 17
9. Selecting the Right Key Lengths 18
10. How to Encrypt a File for a Selected Recipient 19
11. How to Decrypt a File Sent by Another User 22
12. How to Save or Import Configuration Settings 24
13. References 25

# 1. Introduction

- The tool described in this manual is a **public key cryptography application** for the encryption, decryption and digital signature of any type of file to be shared within a group of users. Each user is assumed to have the tool installed on the own computer.
- The tool is **independent from any centralized email server infrastructure**, thus no system administrator or service provider can tap into the encrypted data.
- The tool is based on public key protocols and thus **no preliminary secret key exchange** between users is required.
- The tool is of the **hybrid type** because it uses two distinct protocols:
  - The actual file bytes are encrypted and decrypted with the AES (Advanced Encryption Standard) symmetric cipher using a random session key generated each time a new encryption occurs. This algorithm is very fast and efficient.
  - The AES session key is then encrypted by using the ECC (Elliptic Curve Cryptography) public key scheme.
- Both **AES and ECC algorithms are standard and are recommended by the NSA** (National Security Agency). The present implementation follows the guidelines of NIST (National Institute of Standards and Technology).
- Before operation, the system requires a certain amount of preliminary information to be exchanged among the users: an agreed security level, the type of ECC curve to be adopted and the public key of each user. **This information can be exchanged in a non-secure way**, e.g. by standard email.

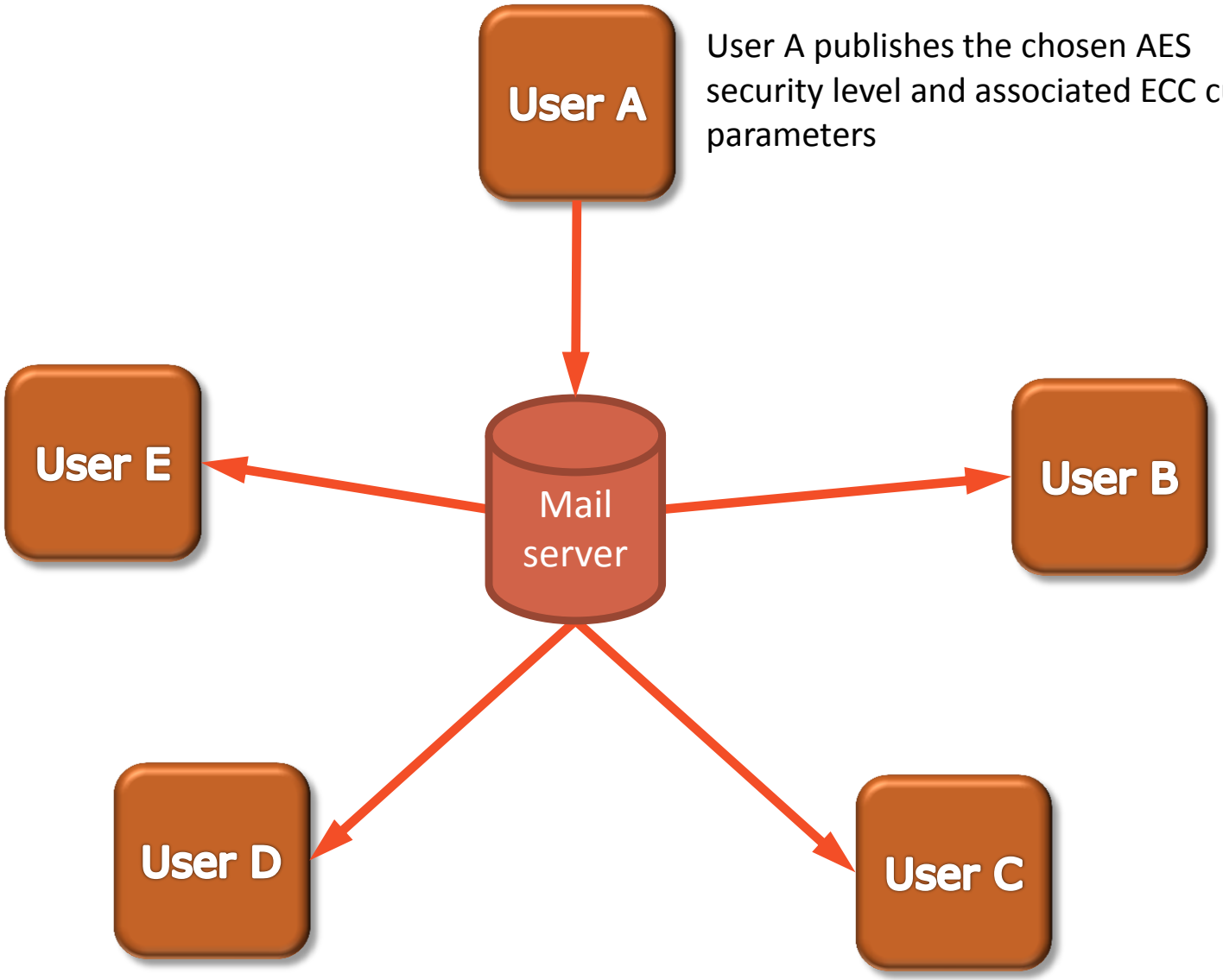
# 1. Introduction - A generic email / webmail system



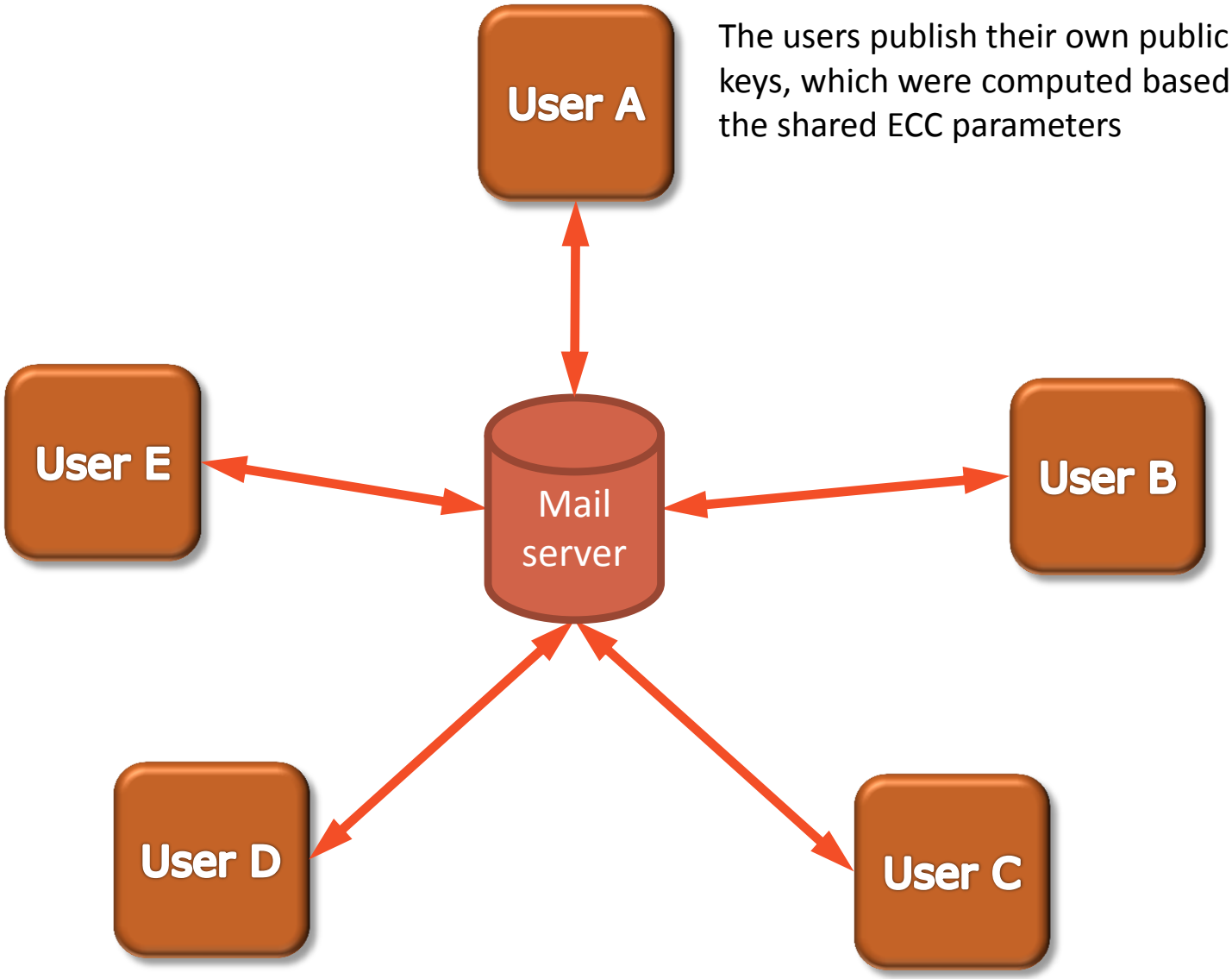

Each user has installed the public encryption tool on his/her computer

Note: all communication channels are assumed insecure

# 1. Introduction - Phase 1: the Master User shares setup parameters



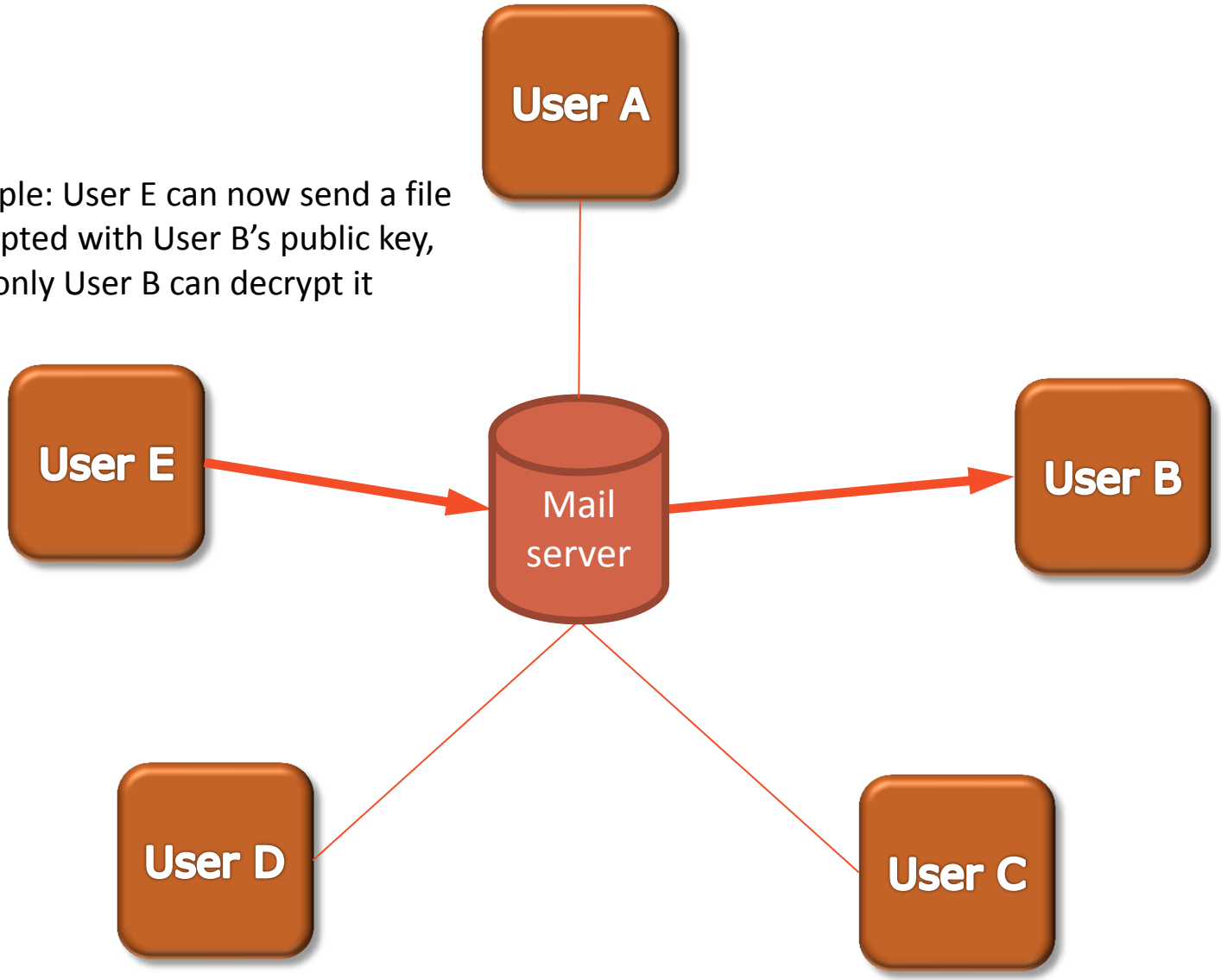
# 1. Introduction - Phase 2: each user shares his / her own public key




The users publish their own public keys, which were computed based on the shared ECC parameters

# 1. Introduction - Phase 3: secure communication between users can start

Example: User E can now send a file encrypted with User B's public key, thus only User B can decrypt it



## 2. Installation and System Requirements

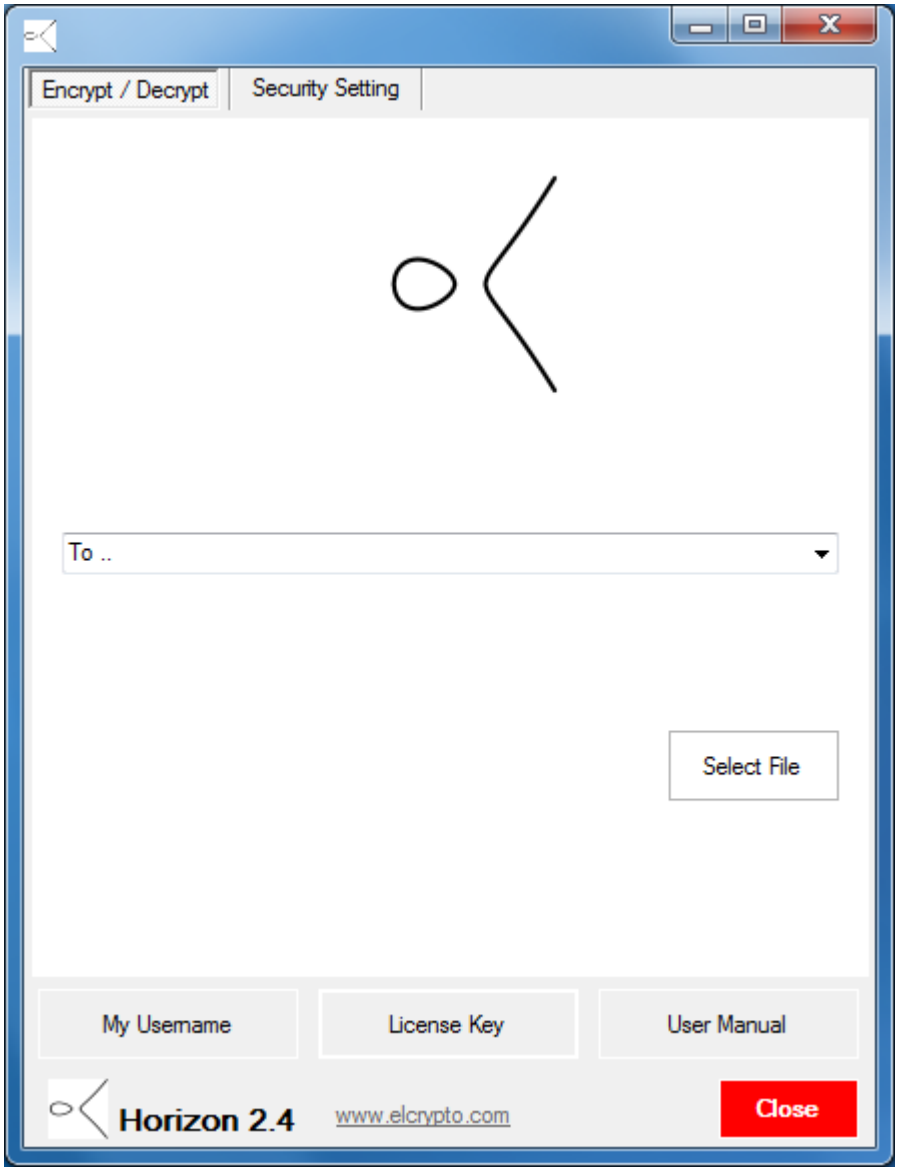
Once you have downloaded the Horizon publishing package, launch **setup.exe** and step through a wizard to install the application. The basic requirement is:

- Microsoft .NET Framework 4 Client Profile (x86 and x64)

If the required Framework is not found on the host computer, the setup wizard will guide the user to a free download of the Framework 4.

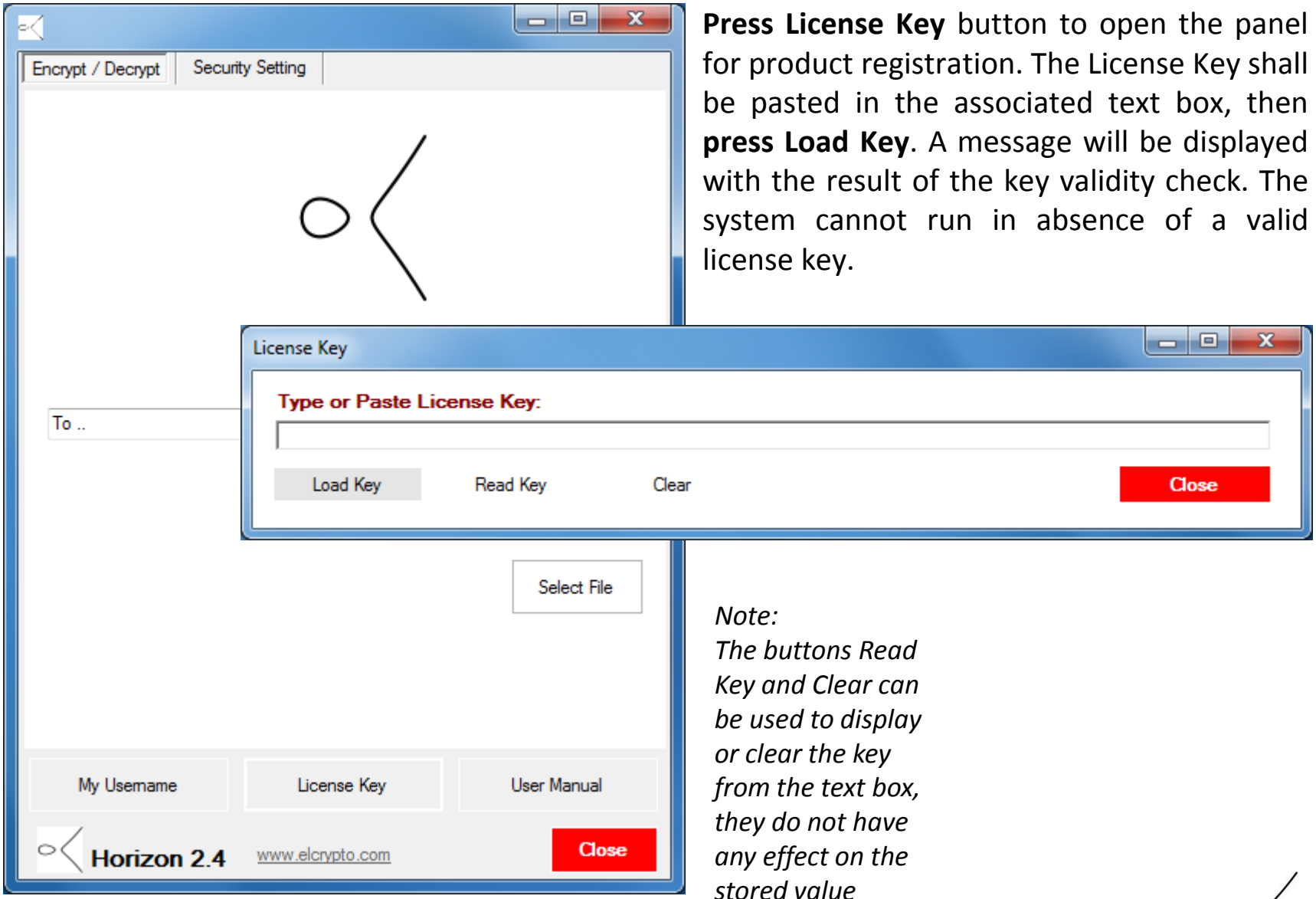
Once the installation is successfully completed, the application Horizon.exe will be accessible from the start menu or through a shortcut on the desktop.

# 3. Opening Screen




**Launch Horizon** (from the Start menu or from the desktop icon) and the interface panel will appear.

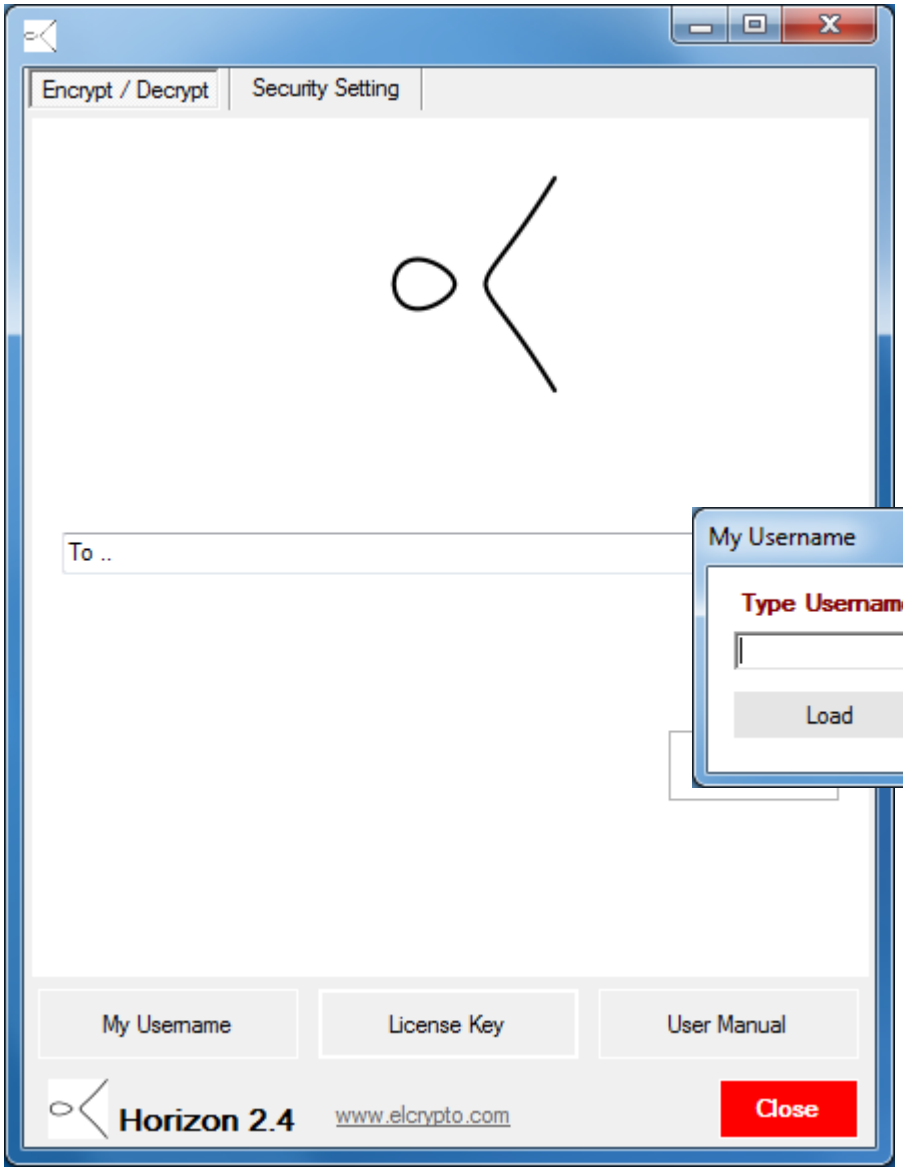
# 4. License Key

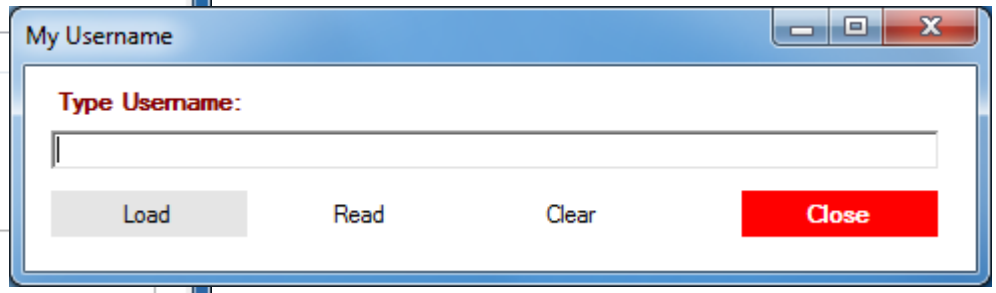



**Press License Key** button to open the panel for product registration. The License Key shall be pasted in the associated text box, then **press Load Key**. A message will be displayed with the result of the key validity check. The system cannot run in absence of a valid license key.

*Note:*
*The buttons Read Key and Clear can be used to display or clear the key from the text box, they do not have any effect on the stored value*

# 5. Entering My Username



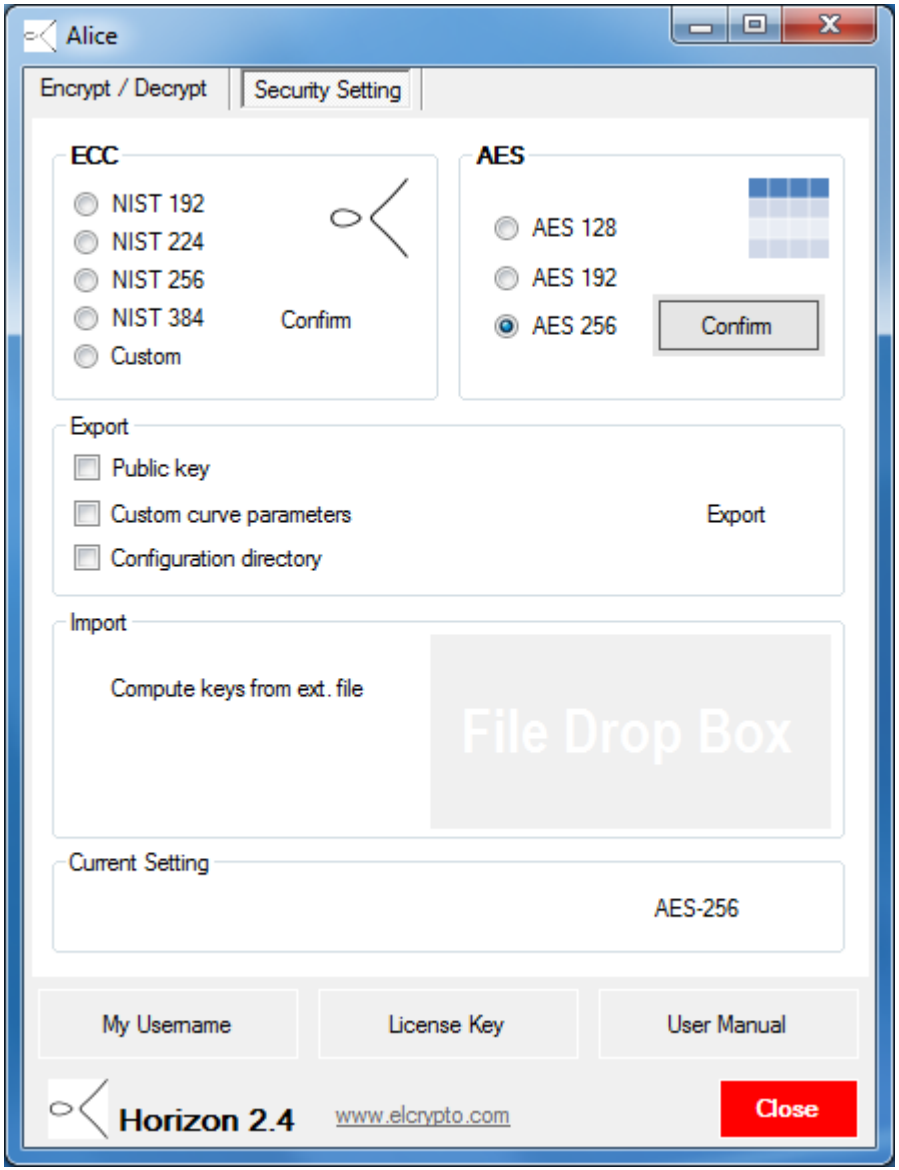




**Press My Username** button to open a panel where your username shall be typed in. This is the name which will be shown to other users. The username shall be written into the associated text box (**MAX 80 char**), then **press Load**. The name will appear on the tool panel upper border.

The system cannot run in absence of a user name.

*Note:*
*The buttons Read and Clear can be used to display or clear the name from the text box, they do not have any effect on the stored value*

# 6. Select an AES Security Level

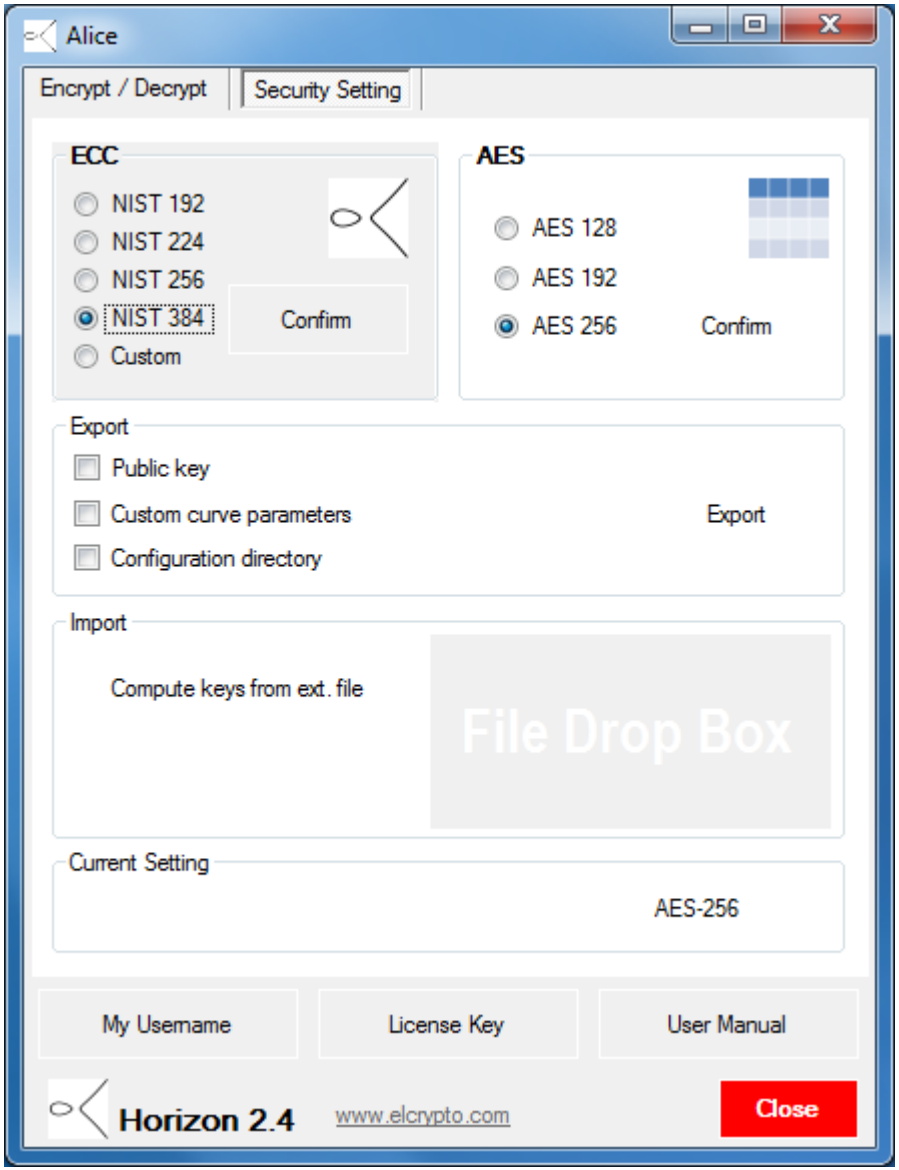



The first thing to do for the Master user is to select a desired level of security, both for the asymmetric (ECC) and for the symmetric (AES) part of the system.

**Select the Security Setting toggle screen** then, for the symmetric part **tick a security level** (e.g. AES-256) **and press Confirm**.

The choice will be displayed below.

# 7. Select a Type of Elliptic Curve




Then one needs to choose the public key encryption method; this is done by selecting **one of the ECC choices.**

There are the following cases:

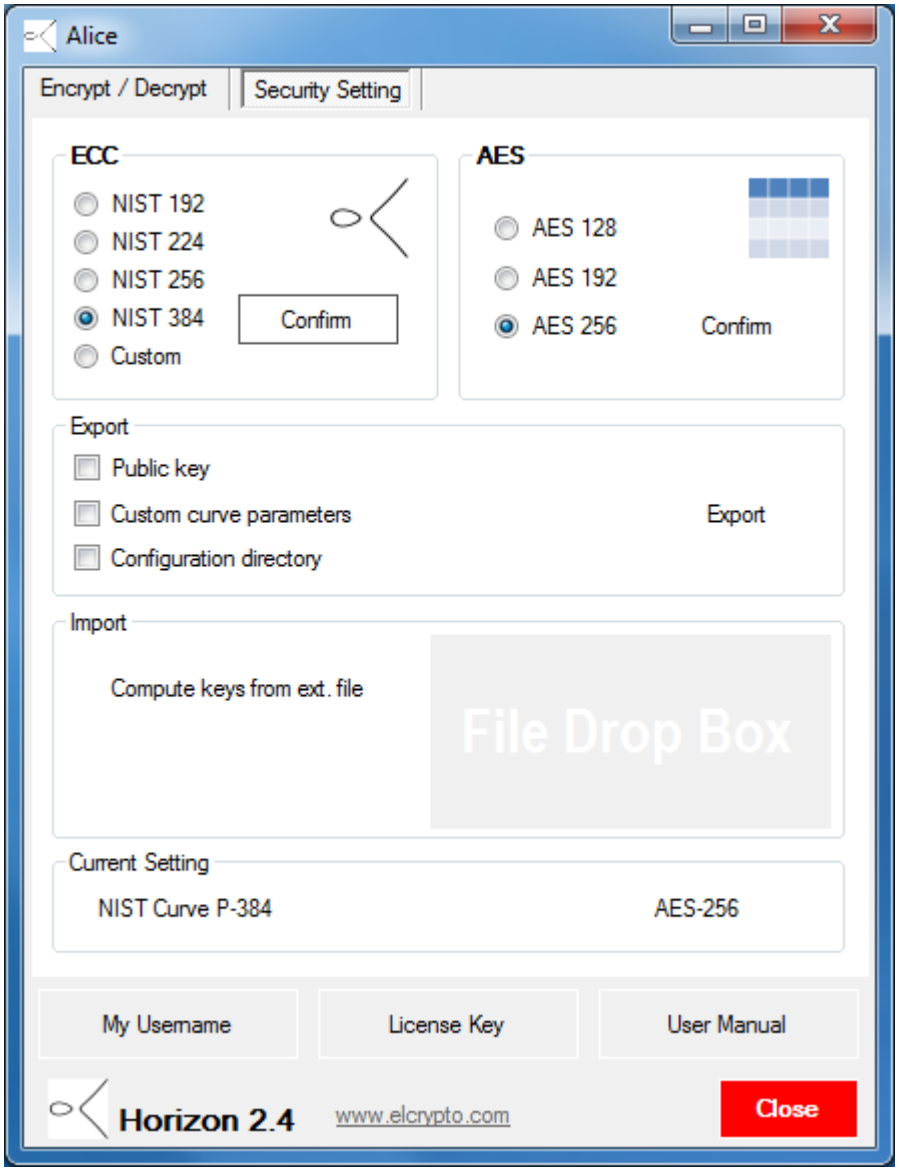
a) one of the standard elliptic curves recommended by NIST,

b) a custom (random) elliptic curve; this case requires a Master User to select a security level and compute the curve parameters. There are two sub-cases:

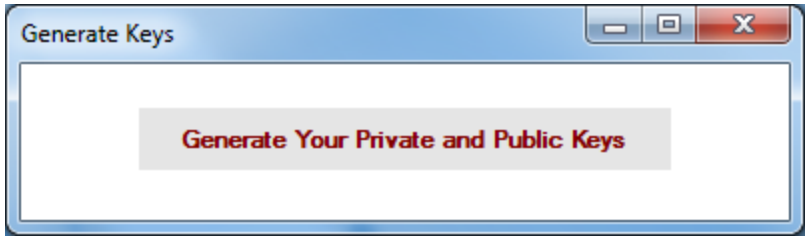
b.1) if you are the Master User, then you must generate and share the curve parameters file,

b.2) if you are not the Master User, then you must load the curve parameters file sent to you by the Master User.

# 7.a NIST Elliptic Curve Setup




**Case a): Tick one of the NIST curves and press Confirm**, a screen will pop-up, asking you to generate your personal keys:

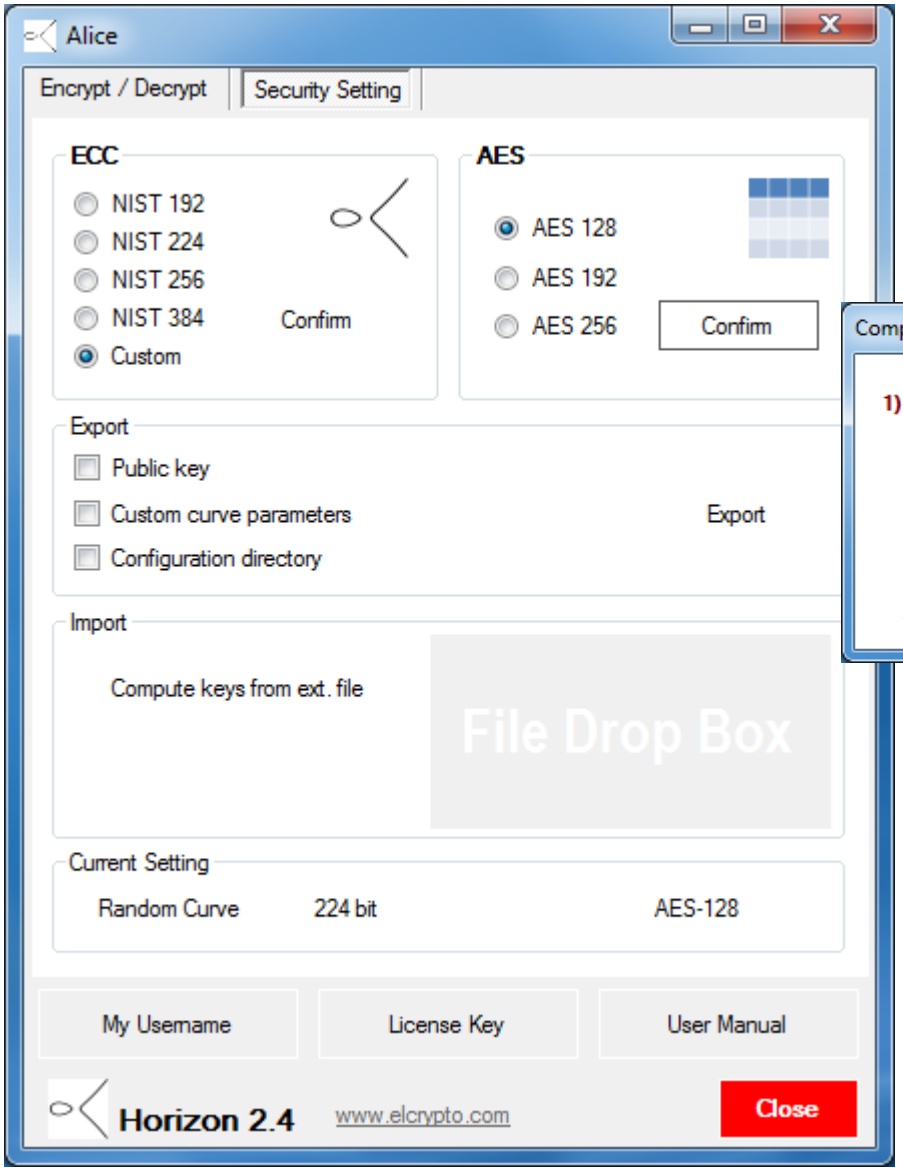



Your username will now appear in the recipient address list of the Encrypt/Decrypt screen.

In order to be able to forward your public key to the other users you shall:

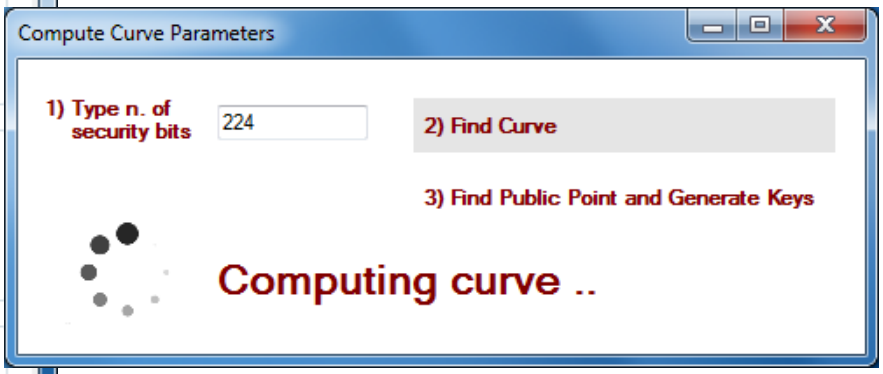
- **Tick Public key** on the **Export panel** and **press Export** button, which will generate the public key file (named **share-public-key.bin**) on the desktop
- Send the file to the other users e.g. by standard email.

# 7.b.1 Random Curve Setup




**Case b.1): Tick Custom and press Confirm**, a screen will pop-up.

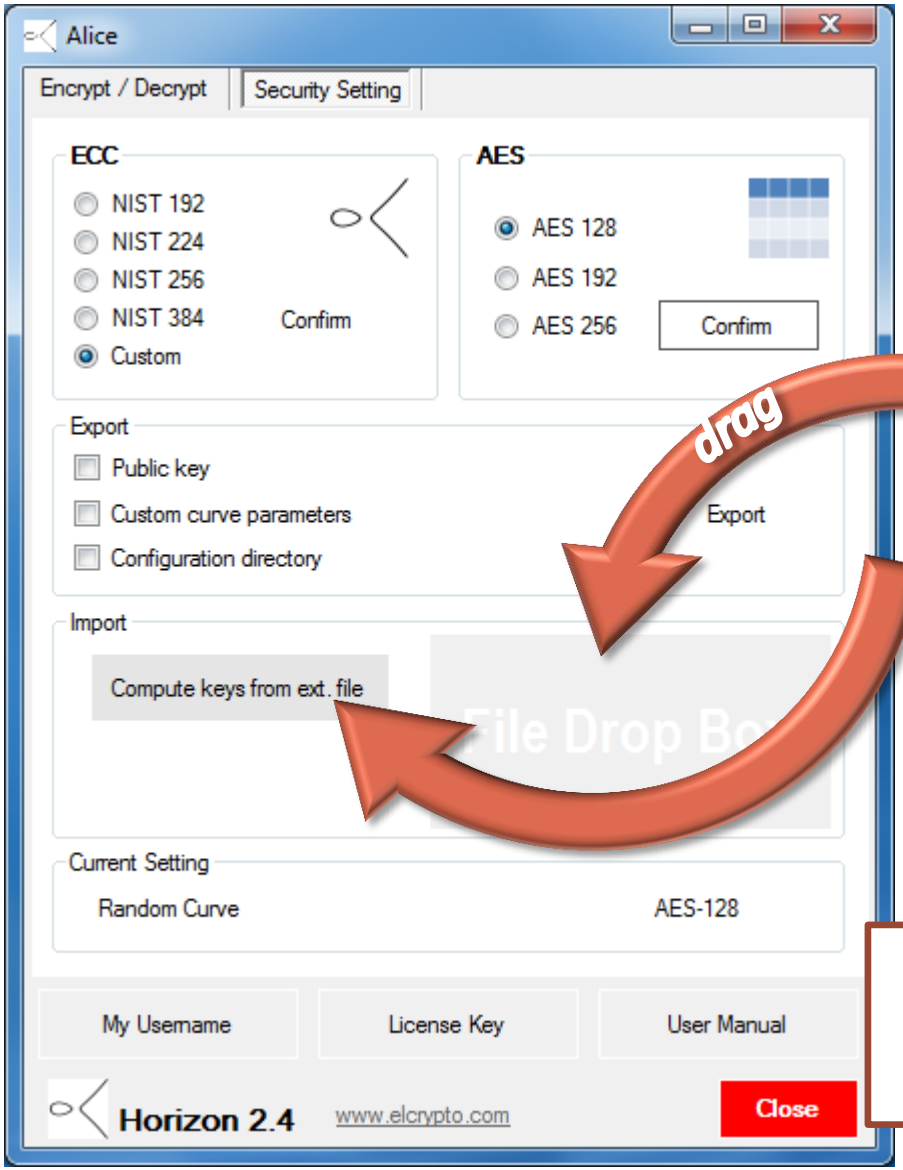
Here you must type the number of security bits, then press buttons 2, 3 in sequence to compute the curve parameters and the personal keys.




Now you need to communicate to the other users both your public key and the curve parameters file:

- **Tick Public key and Custom curve parameters** on the **Export panel** and **press Export** button, which will generate the required files on the desktop
- Send the files **share-param.bin** and **share-public-key.bin** to the other users e.g. by standard email.

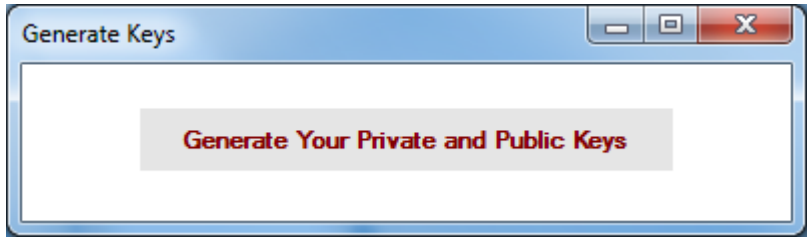
# 7.b.2 Loading Parameters From External File




**Case b.2): Drag and drop** into the grey text box the file **share-param.bin** received from the Master User.

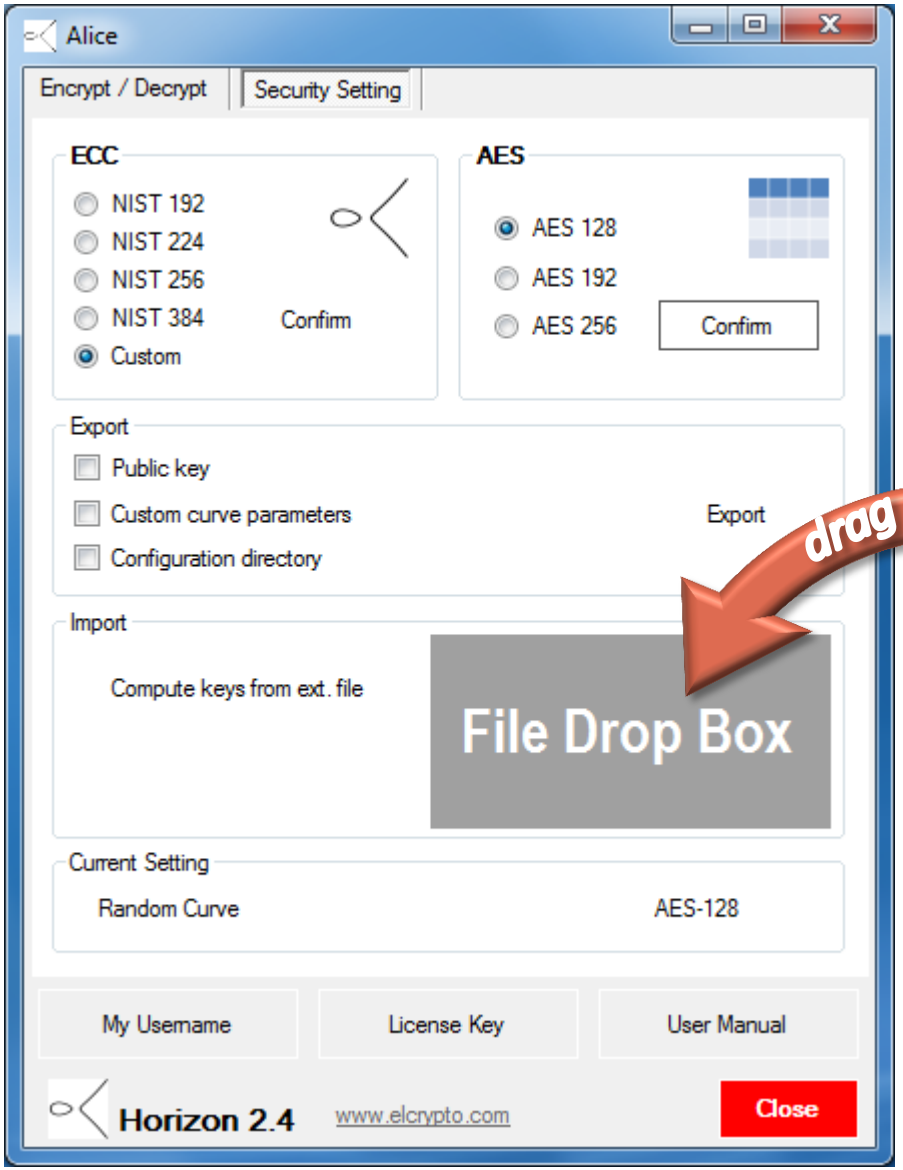
**share-param.bin**

Then click on the button **Compute keys from ext. file**; a screen will pop-up, asking you to generate your keys:




After that, you are ready to share your public key (as illustrated before), as well as load other users' public keys.

# 8. Loading Other Users' Public Keys




**Drag and drop** the file **share-public-key.bin** (received from each user) into the grey text box.

The name of the user will automatically become available in the recipient address list of the Encrypt / Decrypt screen.

**share-public-key.bin**

drag

## 9. Selecting the Right Key Lengths

No matter whether the ECC choice is a random or a NIST curve, in order to have a balanced system the ECC key length **should be twice the length of the AES key.**
The following table suggests balanced combinations:

| Cryptographic Strength | AES key length | ECC key length |
|---|---|---|
| 128 bit | AES-128 | 256 bit |
| 192 bit | AES-192 | 384 bit |
| 256 bit | AES-256 | 512 or 384 bit |

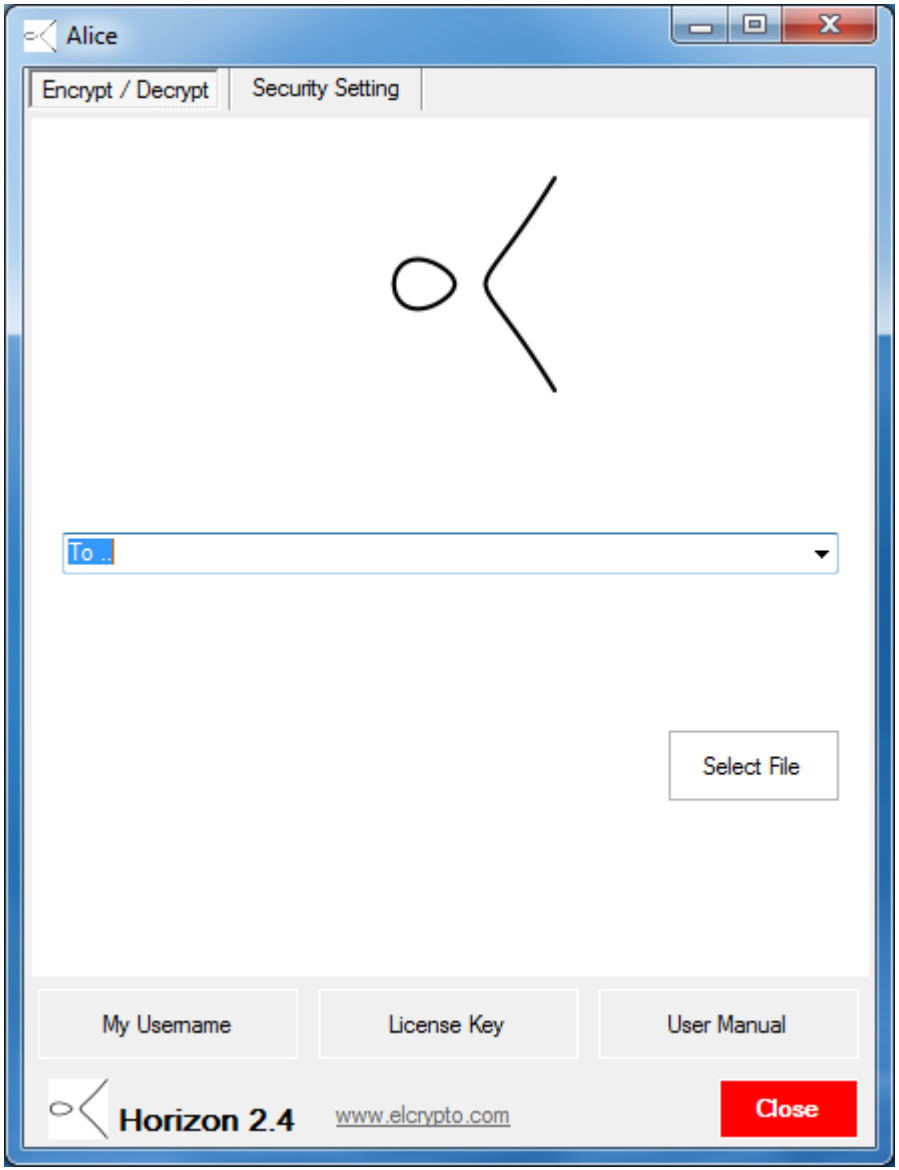
Note that the system will work with any choice, even if unbalanced.

The search for a random curve having the right characteristics is a **complex operation which may take several minutes** for ECC key lengths above about 200 bit.

**Recommended choices:**

- **AES 128 with NIST curve P-256 (adopted by NSA up to SECRET)**
- **AES 192 with NIST curve P-384 (adopted by NSA up to TOP SECRET)**

# 10. How to Encrypt a File for a Selected Recipient - 1

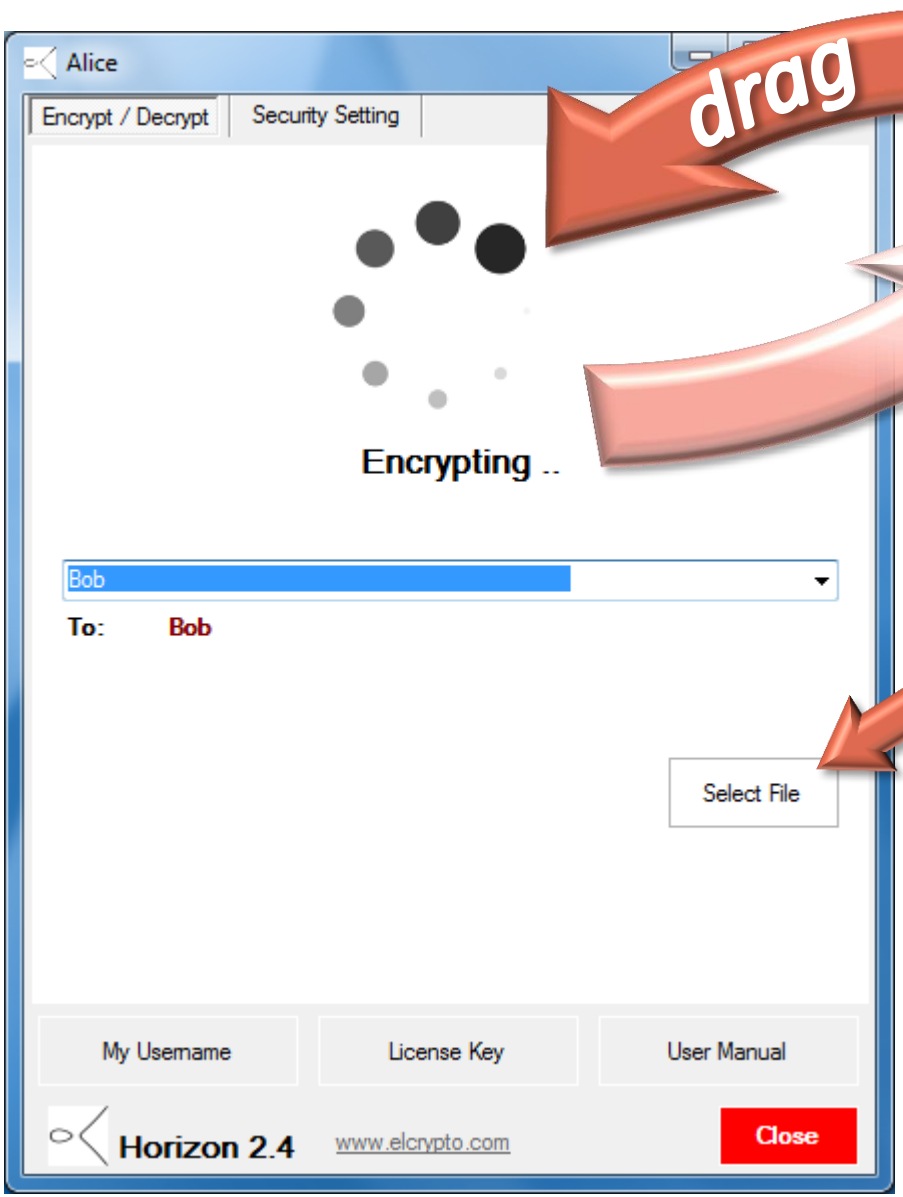



After having performed the setup and having populated the address directory with a list of recipients, **we are now ready to use the tool** to securely exchange files.

**The first thing to do is to select a recipient** of the file we intend to encrypt. This will be the only user able to decrypt the file.

The combo box in the interface allows this selection as shown at left.

# 10. How to Encrypt a File for a Selected Recipient - 2




There are two ways to encrypt / decrypt a file:

a) By **dragging** the file into the curve picture. If the file extension ends with .ecrypt.bmp it will be decrypted, otherwise it will be encrypted.

b) By using the **Select File** button which will open a file manager dialog box for the selection of the file, then by pressing the relevant button for encryption (which will appear after file selection).

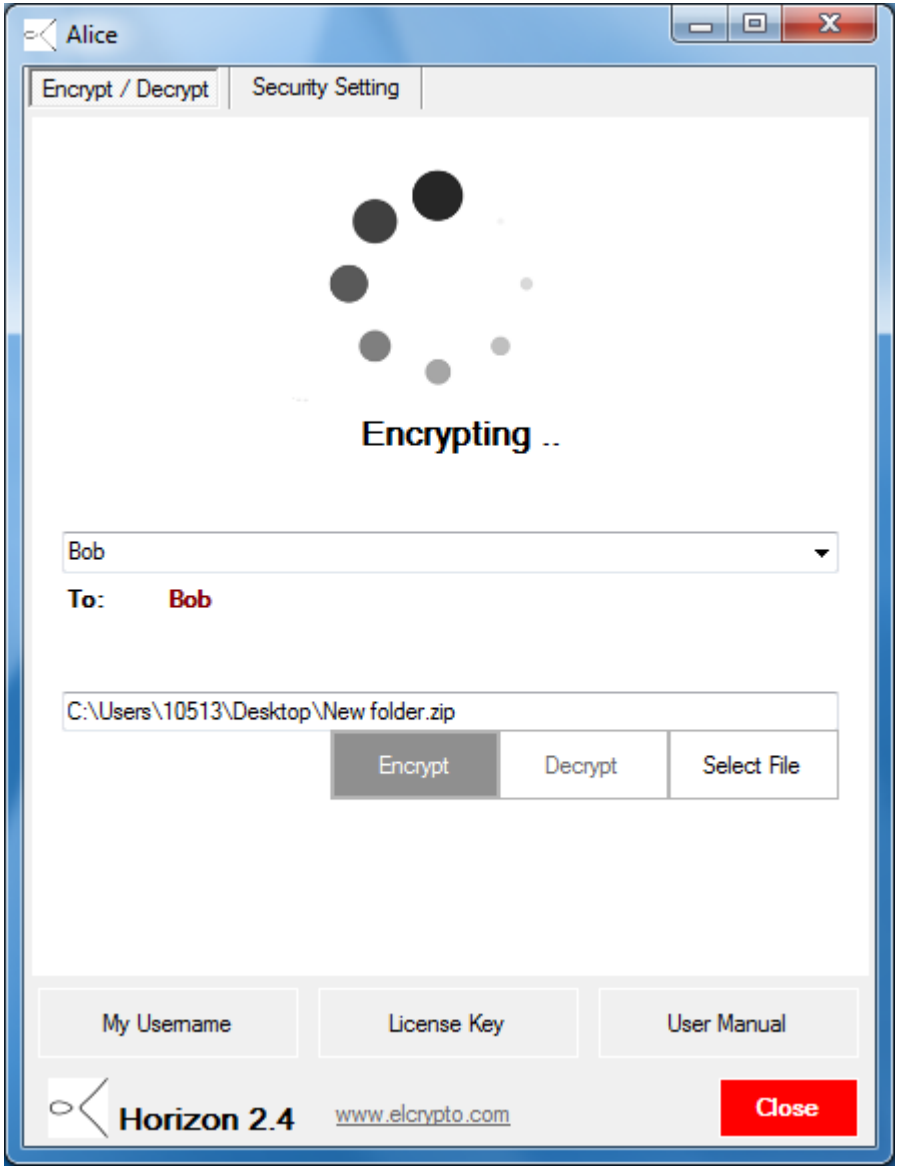
The encrypted version of the file will be created in the same directory of the original file.

The extension of the encrypted file is the same as the original one plus the suffix **.ecrypt.bmp** appended, as it is also transformed into a bitmap.

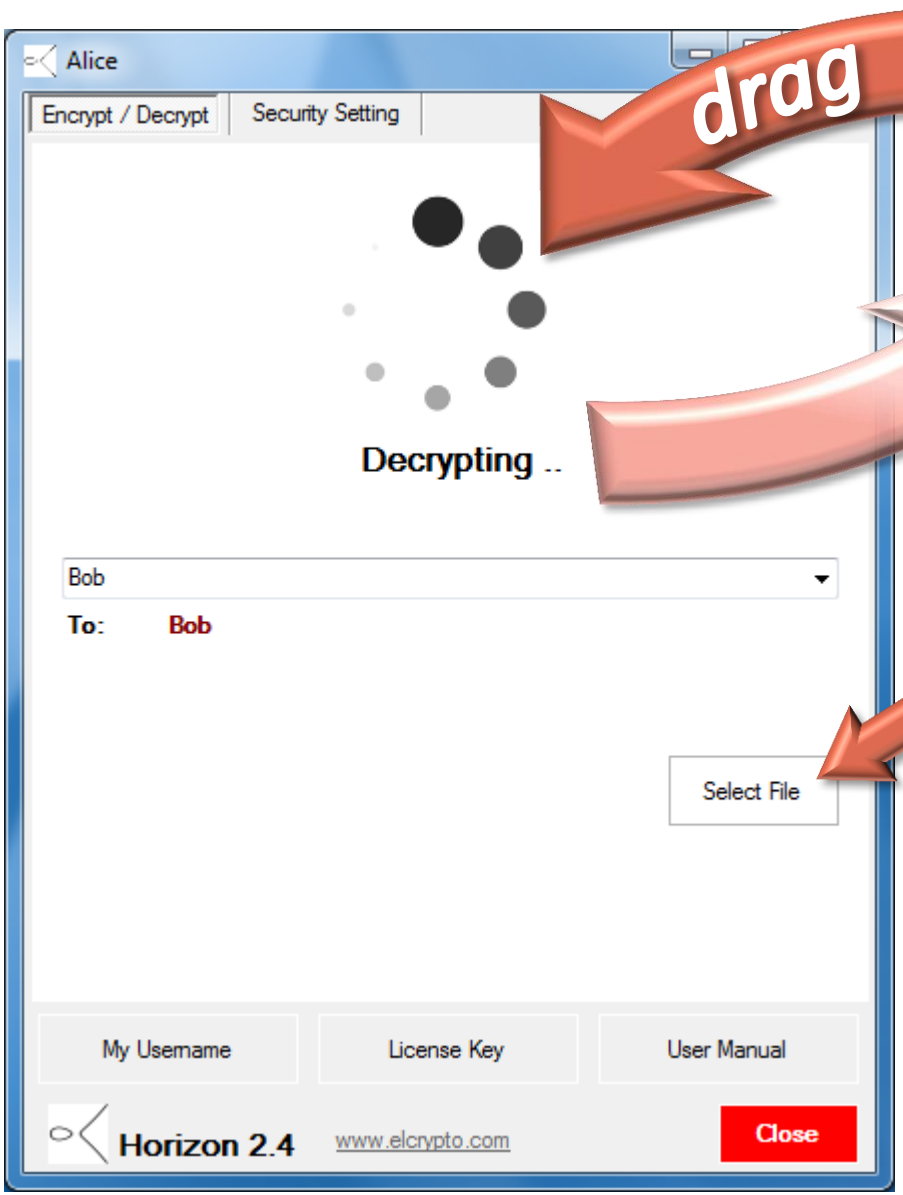
Now the encrypted file is ready to be sent to the selected recipient who is the only one who will be able to decrypt it.

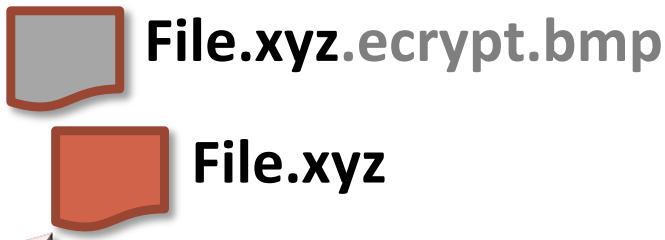
# 10. How to Encrypt a File for a Selected Recipient - 3

Encryption mode b)



# 11. How to Decrypt a File Sent by Another User - 1



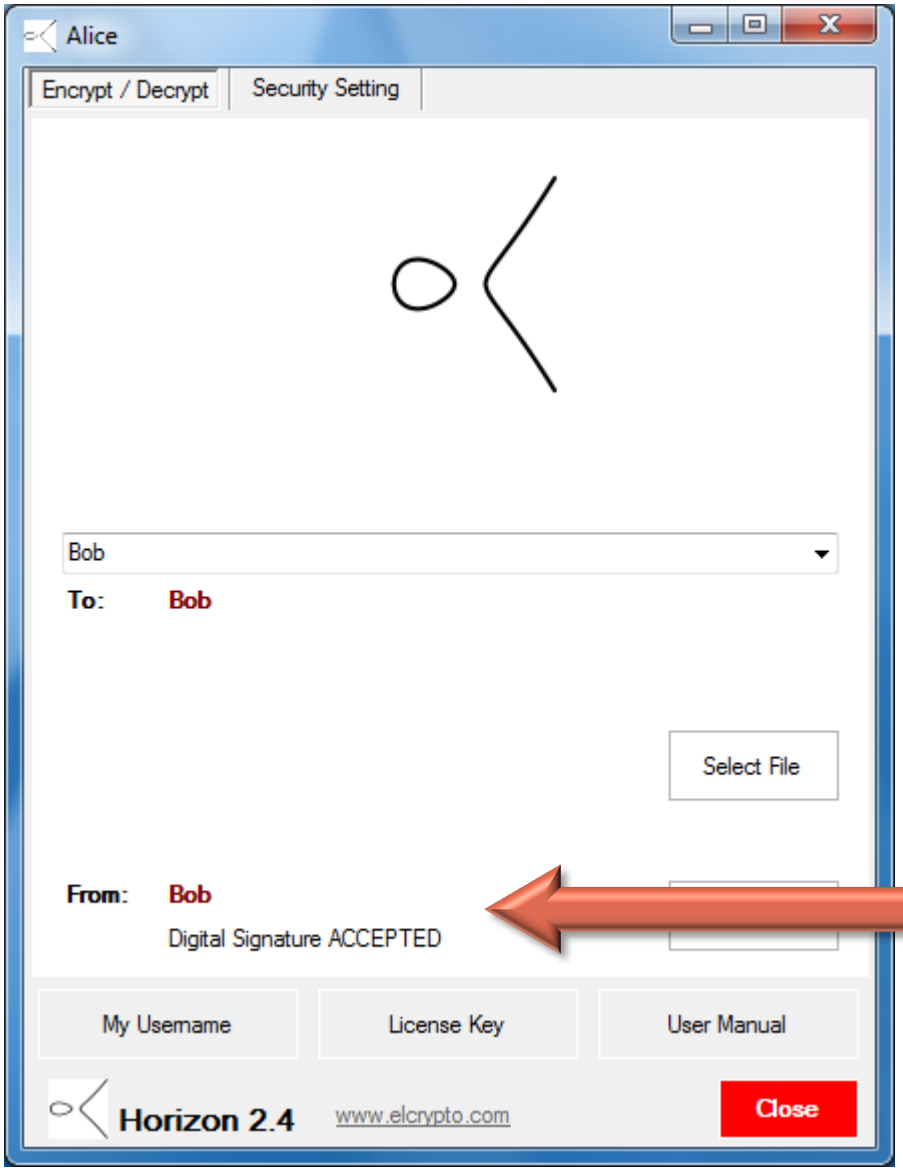

Again, there are two ways of selecting a file for decryption:

a) By **dragging** the encrypted file (suffix .ecrypt.bmp) into the curve picture.

b) By using the **Select File** button which will open a file manager dialog box for the selection of the file, then by pressing the relevant button for decryption.

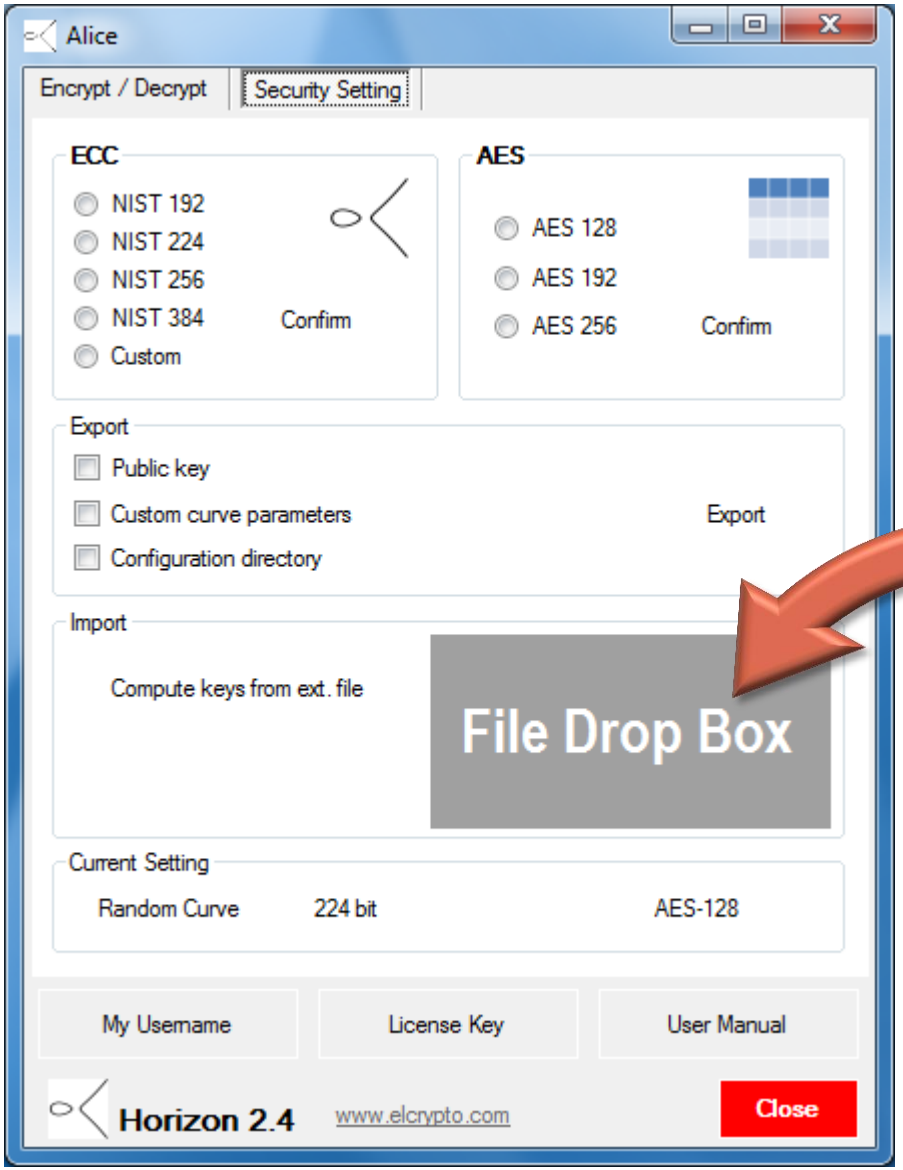
The decrypted version of the file will be created in the same directory as the original file.

# 11. How to Decrypt a File Sent by Another User - 2




The interface panel will show the **sender identity** and the result of the digital signature verification.

# 12. How to Save or Import Configuration Settings




In order to install the tool on another computer without having to re-set and re-load all the public keys of the users, one can export the whole configuration directory (Conf) by selecting the appropriate tick box in the Export panel and by pressing Export.

The Conf directory will be generated on the desktop.

The configuration can then be reloaded by dragging the Conf folder into the grey box.


This feature is useful also in case one wants to switch among different configurations (e.g. different security levels for different user groups).

# 13. References

Algorithms for: random number generation, cipher modes of operation, private / public key encryption, decryption and digital signature are based on the following standards and publications.

**Federal Information Processing Standards:**

- FIPS 186-3: DIGITAL SIGNATURE STANDARD (DSS)
- FIPS 197: Announcing the ADVANCED ENCRYPTION STANDARD (AES)
- FIPS 180-2: Announcing the SECURE HASH STANDARD

**NIST (National Institute of Standards and Technology) publications:**

- NIST Special Publication 800-38A Recommendation for Block Cipher Modes of Operation, Methods and Techniques, 2001 Edition
- NIST Special Publication 800-90: Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised), March 2007
- NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms, January 31, 2005