NAMIBIA CYEBR SECURITY INCIDENT RESPONSE TEAM
(NAM-CSIRT)

Pretty Good Privacy (PGP)
Email Encryption Guideline

Contents

1. Kleopatra Installation Guide

1.1 Download the Gpg4win package from the official website: https://gpg4win.org.

1.2 Run the downloaded installer and follow the on-screen instructions, selecting the Kleopatra installation option.
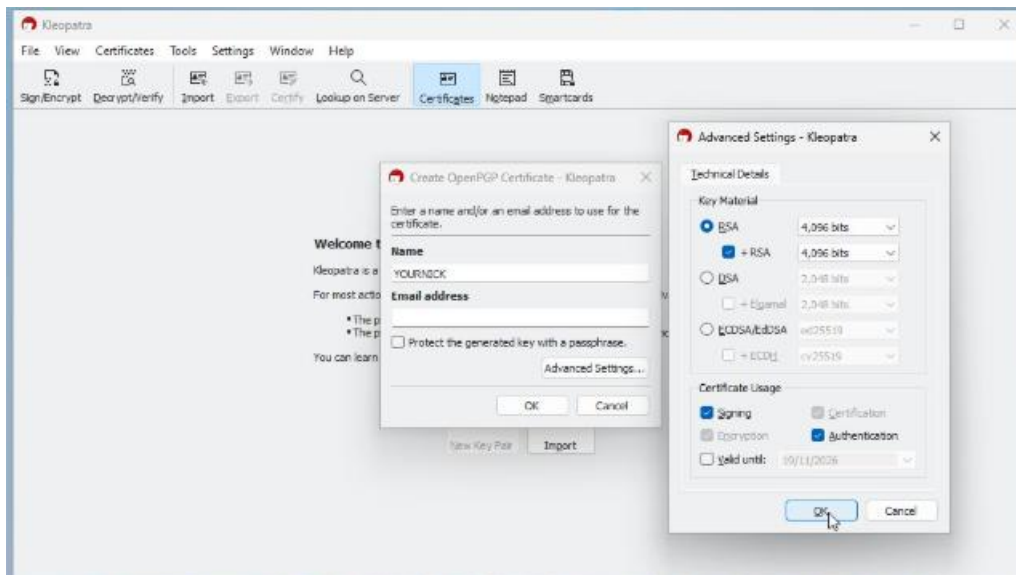
1.3 Ensure the following components are installed: GnuPG, Kleopatra, GpgOL, GpgEX.

2. Generating keys in Kleopatra

2.1 Open the Kleopatra application and click the *New Key Pair* button and follow the instruction.
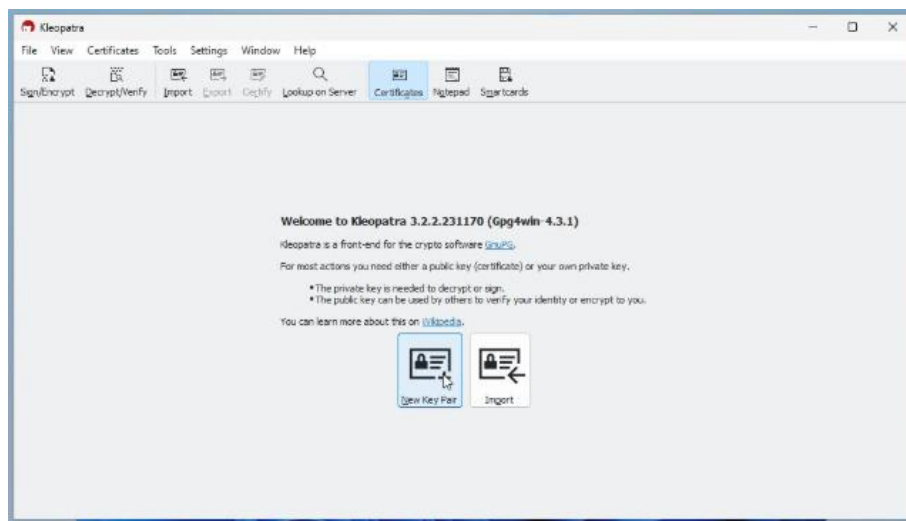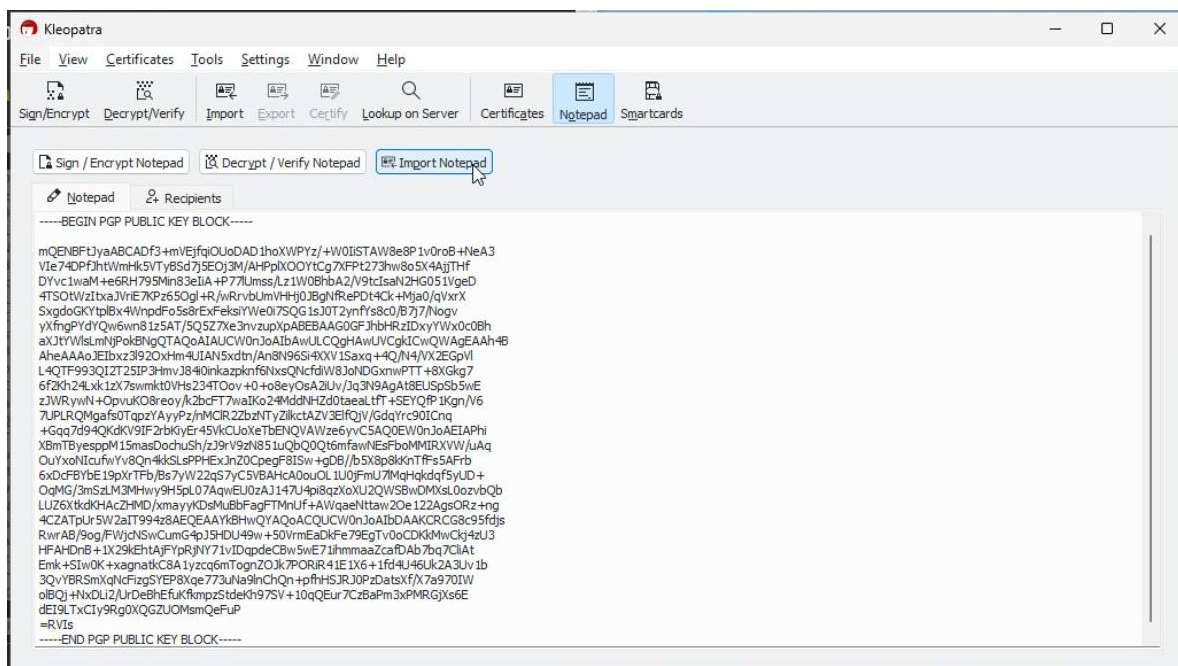

2.2 Select your preferred key algorithm and size *RSA, 4096 bits*, check the *Authentication* option, and click *OK*.

3. Importing public keys in Kleopatra

3.1 Download and Open text file containing the public key.

3.2 Open the Kleopatra application and select the Notepad option.

3.3 Paste the public key and click Import Notepad.

4. Encrypting messages in Kleopatra

4.1 Open the Kleopatra application and click *Notepad*, then paste/type the content of the message you want to encrypt into the text field.

4.2 Select the recipient's public key from the list of available keys.
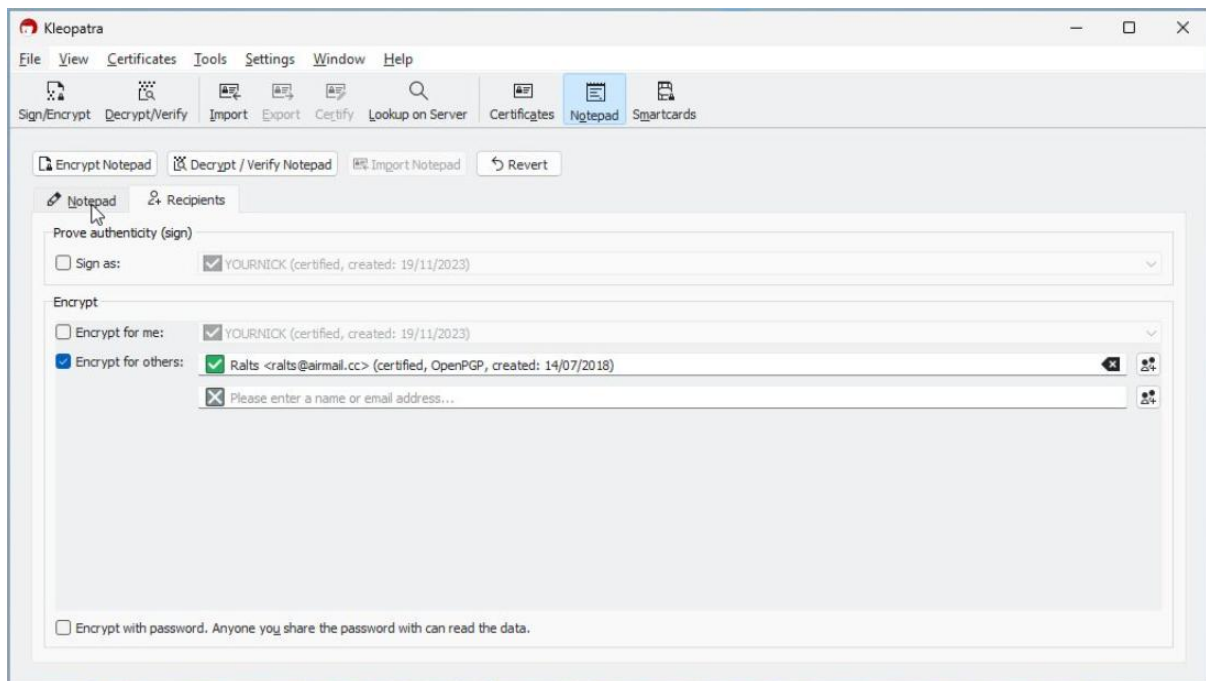
4.3 Click Encrypt Notepad.

4.4 After encrypting the message, copy the resulting text to the clipboard and share via email

Note, we do not need to import the public key again when encrypting the next messages. The key will be saved in the program files.
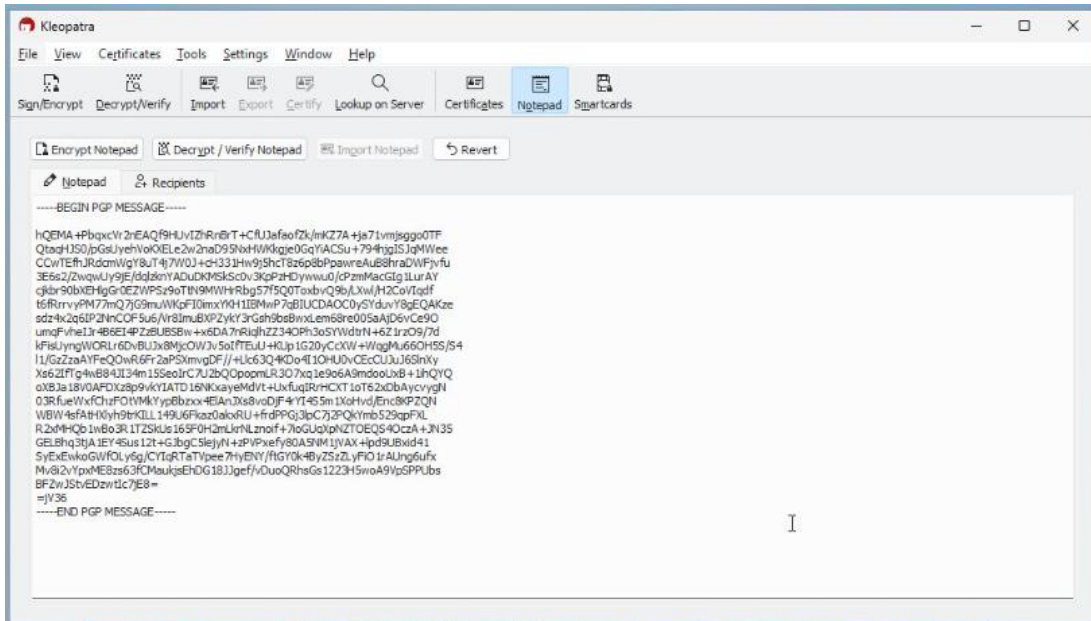
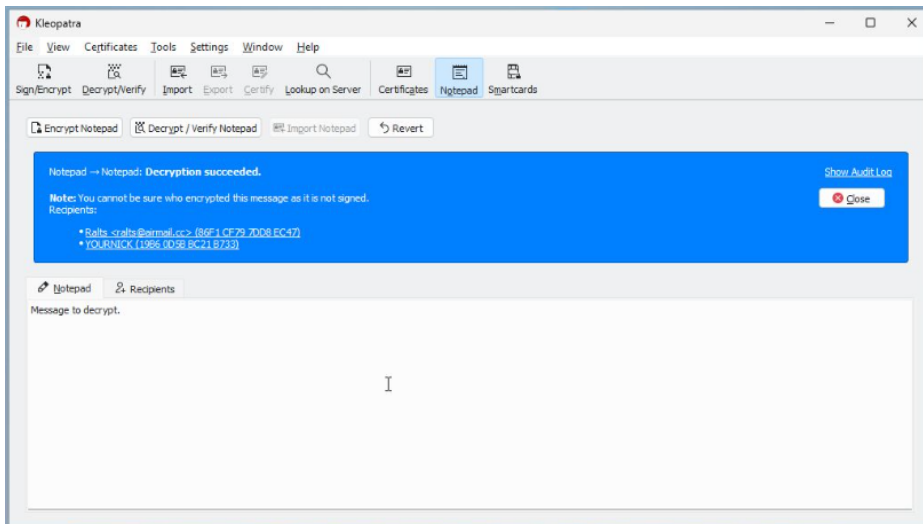# 5. Decrypting messages in Kleopatra

5.1 Open the encrypted message.

5.2 Copy the encrypted text to the clipboard, then open the Kleopatra application.

5.3 Click Notepad and paste the encrypted text.

5.4 Click *Decrypt / Verify Notepad*.

6. Decrypted message

_____The End_____