https://docs.oracle.com/cd/E88140_01/books/Secur/secur_dataencrypt007.htm

About Key Exchange for RSA Encryption
If you are using RSA encryption for communications between Mobile Web Clients and the Siebel Remote Server, then the following steps explain how Siebel encryption keys are exchanged between the client and the server:

The client generates a private/public key pair. The public key is sent as part of the Hello message to the remote server.

When the server receives a Hello message, it generates an AES-based symmetrical session key and encrypts the symmetrical session key using the client's public key from the Hello message. The encrypted session key is sent back to the client as part of the Hello Acknowledge message.

The client uses its private key to decrypt the server-generated session key. From this point on, both the client and the server use the server-generated session key to encrypt and decrypt messages.

The session key is good for the lifetime of the connection.

Bitmap (BMP)

BMP is a standard format used by Windows to store device-independent and application-independent images. The number of bits per pixel (1, 4, 8, 15, 24, 32, or 64) for a given BMP file is specified in a file header. BMP files with 24 bits per pixel are common.

https://learn.microsoft.com/en-us/windows/win32/gdiplus/-gdiplus-types-of-bitmaps-about

Standaard Opslag

Nodig in de app:

1.1.1 Als gebruiker kan ik een folder instellen via een menu als standaard folder om al de AES-sleutels in op te slaan. Deze folder wordt automatisch gebruikt voor het laden en opslaan van sleutels.

1.1.2 Als gebruiker kan ik AES-sleutel en IV genereren en automatisch wegschrijven in een folder. Beide worden opgeslagen als een **base64** string in een bestand. *(Welke*

→ standaard folder voor gegenereerde AES-sleutels (.txt => base64 string)

1.1.3 Als gebruiker kan ik een RSA key pair genereren. Beide sleutels worden opgeslagen in **XML-formaat**.

→ standaard folder voor RSA PUBLIC sleutels (XML)
standaard folder voor RSA PRIVATE sleutels (XML)

1.2.3 Als gebruiker kan ik een folder instellen via een menu als standaard folder om al de ciphertext in weg te schrijven. De inhoud van deze folder wordt automatisch getoond tijdens het selecteren van een ciphertext bij het decryptie proces.

→ standaard folder voor AES-encrypted images (.txt)

1.2.4 Als gebruiker kan ik een folder instellen via een menu als standaard folder om al de **plaintext (afbeeldingen)** in weg te schrijven.

→ standaard folder voor images (.bmp)

1.3.3 Als gebruiker kan ik een folder instellen via een menu als standaard folder om al de ciphertext AES keys in weg te schrijven. De inhoud van deze folder wordt automatisch getoond tijdens het selecteren van een ciphertext bij het decryptie proces. Maak vervolgens ook een onderscheid tussen oorspronkelijk gegenereerde AES-sleutels en gedecrypteerde AES-sleutels.

→ standaard folder voor RSA-encrypted AES-keys (.txt)
standaard folder voor RSA- DEcrypted AES-keys (.txt)

Flow AES encryptie

1.2.1 Als gebruiker kan ik een AES-sleutel selecteren om een **encryptie** mee uit te voeren. De sleutels van de standaard folder (1.1.1) worden binnen de WPF-applicatie getoond.

1.2.5 Als gebruiker kan ik een afbeelding selecteren van een bepaalde extensie om te encrypteren. *(Welke afbeelding extensie hebben jullie gekozen voor jullie applicatie?)*

1.2.7 Als gebruiker kan ik op een encrypteer-knop klikken om het encryptie proces te starten.

1.2.9 Als gebruiker kan ik de naam van het bestand kiezen om de ciphertext in op te slaan die geproduceerd is na encryptie. De ciphertext wordt als een **base64** string opgeslagen in het bestand.

Flow AES DEcryptie

1.2.2 Als gebruiker kan ik een AES-sleutel selecteren om een **decryptie** mee uit te voeren. De sleutels van de standaard folder (1.1.1) worden binnen de WPF-applicatie getoond.

1.2.6 Als gebruiker kan ik een keuze maken om een ciphertext te decrypteren als een afbeelding van de gekozen extensie.

1.2.8 Als gebruiker kan ik op een decrypteer-knop klikken om een decryptie proces te starten.

1.2.10 Als gebruiker kan ik de naam van het bestand kiezen om de nieuwe plaintext (afbeelding) in op te slaan die geproduceerd is na decryptie.

1.2.11 Behandel **CryptographicExceptions** en waarschuw de gebruiker bij het gebruik van verkeerde keys.

https://learn.microsoft.com/en-us/dotnet/api/system.security.cryptography.aes?view=netframework-4.8.1

Flow RSA Encryptie

1.3.1 Als gebruiker kan ik **asymmetrische public key** selecteren om een **encryptie** mee uit te voeren. De sleutels van de standaard folder (1.1.1) worden binnen de WPF-applicatie getoond.

1.3.4 Als gebruiker kan ik een plaintext AES-sleutel selecteren om later te encrypteren.

1.3.8 Als gebruiker kan ik de naam van het bestand kiezen om de ciphertext in op te slaan die geproduceerd is na encryptie. De ciphertext wordt als een **base64** string opgeslagen in het bestand.

1.3.6 Als gebruiker kan ik op een encrypteer-knop klikken om het encryptie proces te starten.

Flow RSA DEcryptie

1.3.2 Als gebruiker kan ik **asymmetrische private key** selecteren om een **decryptie** mee uit te voeren. De sleutels van de standaard folder (1.1.1) worden binnen de WPF-applicatie getoond.

1.3.5 Als gebruiker kan ik een ciphertext AES-sleutel selecteren om later te decrypteren.

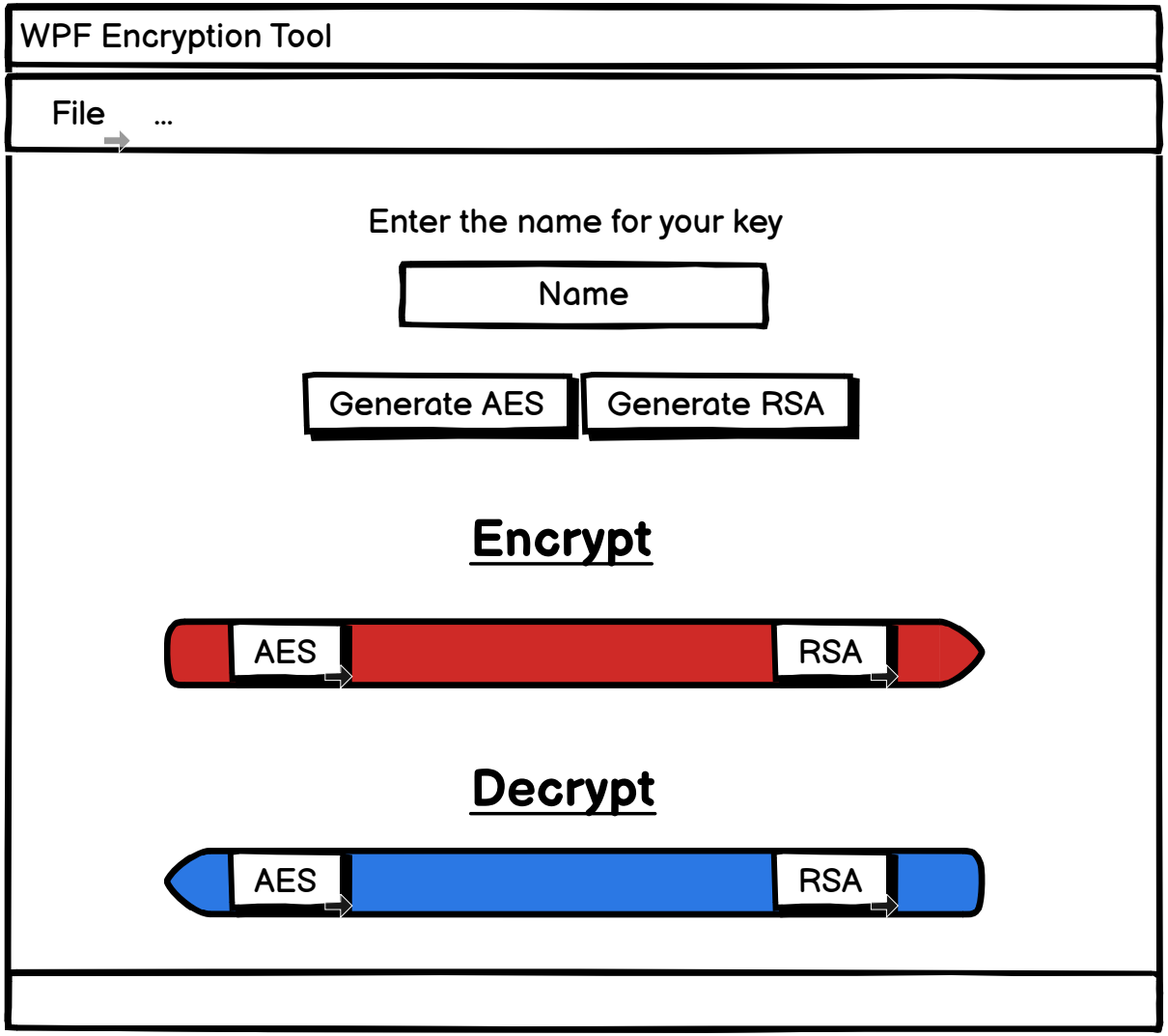
1.3.9 Als gebruiker kan ik de naam van het bestand kiezen om de nieuwe plaintext (AES key) in op te slaan die geproduceerd is na decryptie.

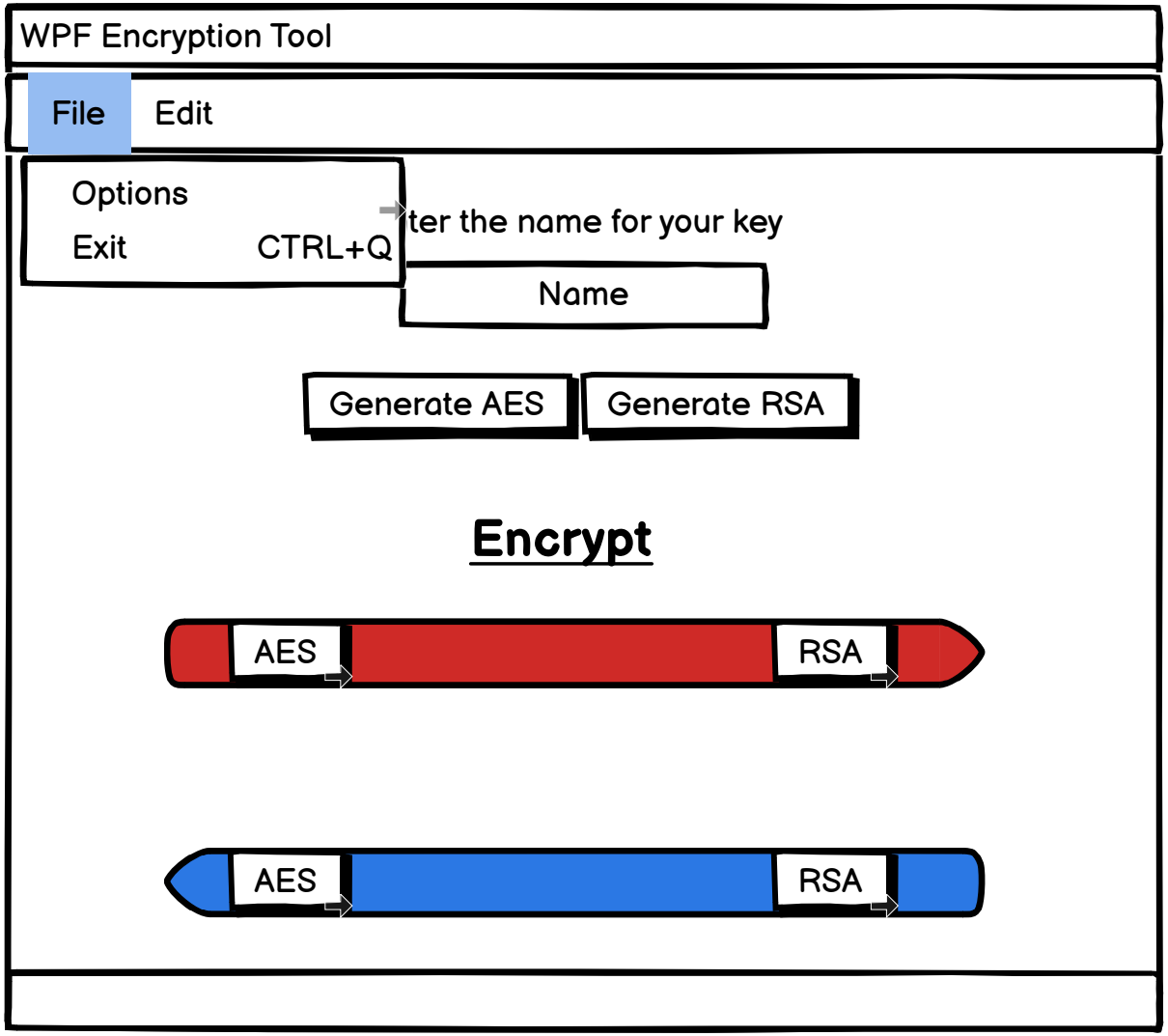
1.3.7 Als gebruiker kan ik op een decrypteer-knop klikken om een decryptie proces te starten.

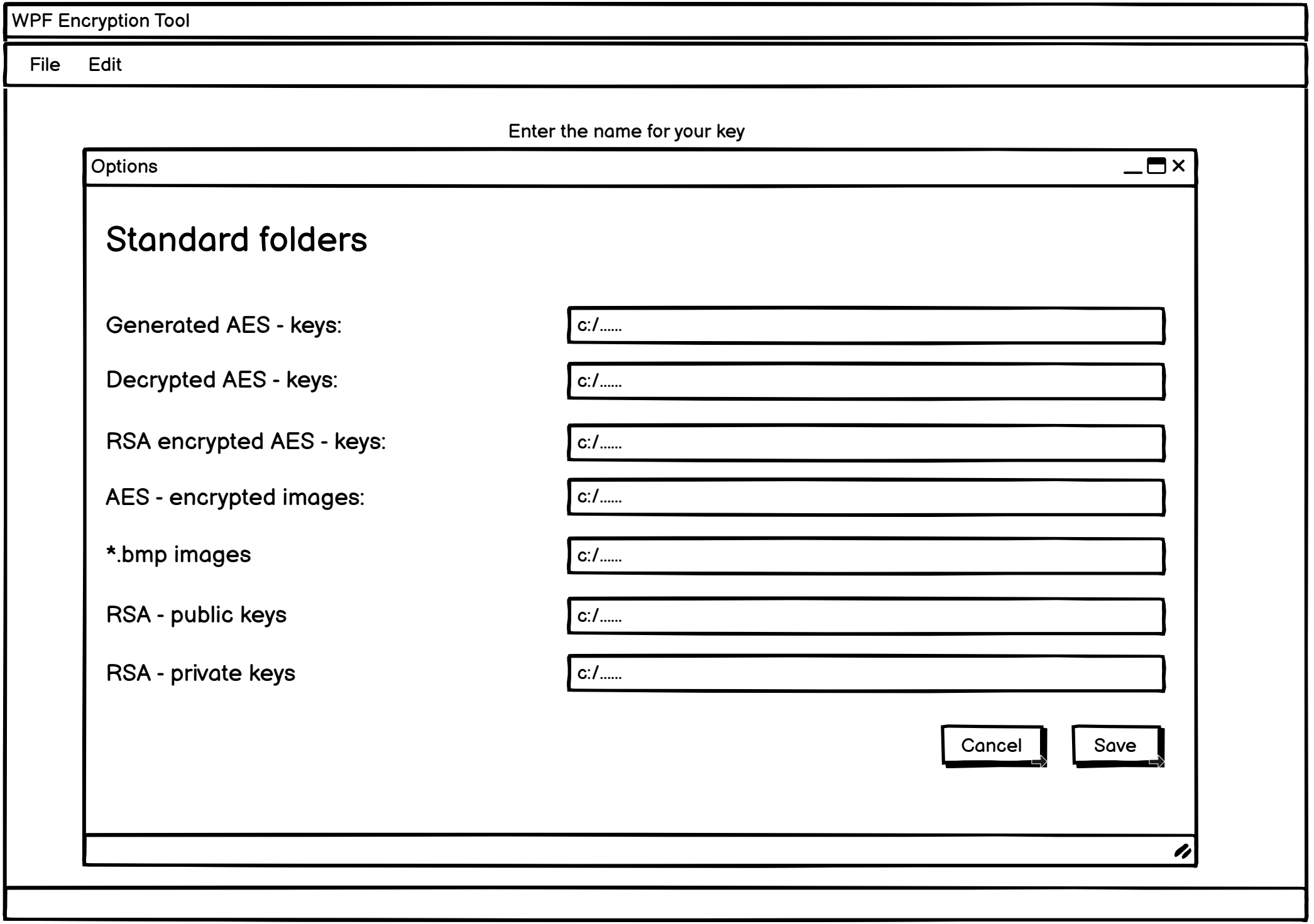
1.3.10 Behandel **CryptographicExceptions** en waarschuw de gebruiker bij het gebruik van verkeerde keys.

https://learn.microsoft.com/en-us/dotnet/api/system.security.cryptography.rsa?view=netframework-4.8.1

FileHelper voor het schrijven en lezen van text bestanden https://www.nuget.org/packages/EasyTextFile


WPF Encryption Tool
File
...
Enter the name for your key
Name
Generate AES
Generate RSA
Encrypt
AES
RSA
Decrypt
AES
RSA


WPF Encryption Tool
File
Edit
Options
Exit
CTRL+Q
ter the name for your key
Name
Generate AES
Generate RSA
Encrypt
AES
RSA
AES
RSA


WPF Encryption Tool
File
Edit
Enter the name for your key
Options
Standard folders
Generated AES - keys:
c:/.....
Decrypted AES - keys:
c:/.....
RSA encrypted AES - keys:
c:/.....
AES - encrypted images:
c:/.....
*.bmp images
c:/.....
RSA - public keys
c:/.....
RSA - private keys
c:/.....
Cancel
Save

WPF Encryption Tool

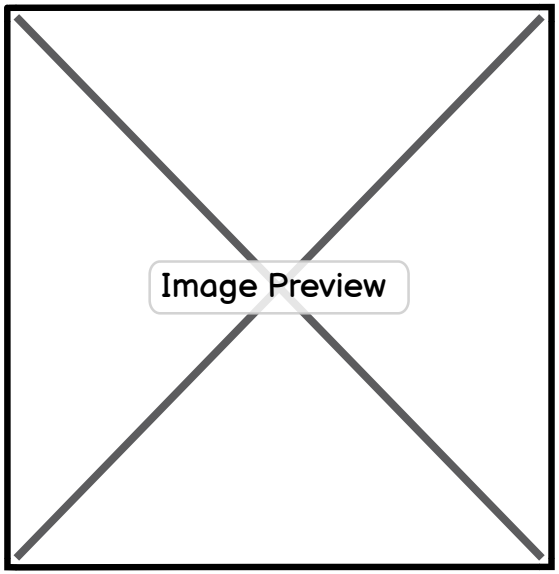
File ...

AES - Encryption

Select AES-encryption key: Key

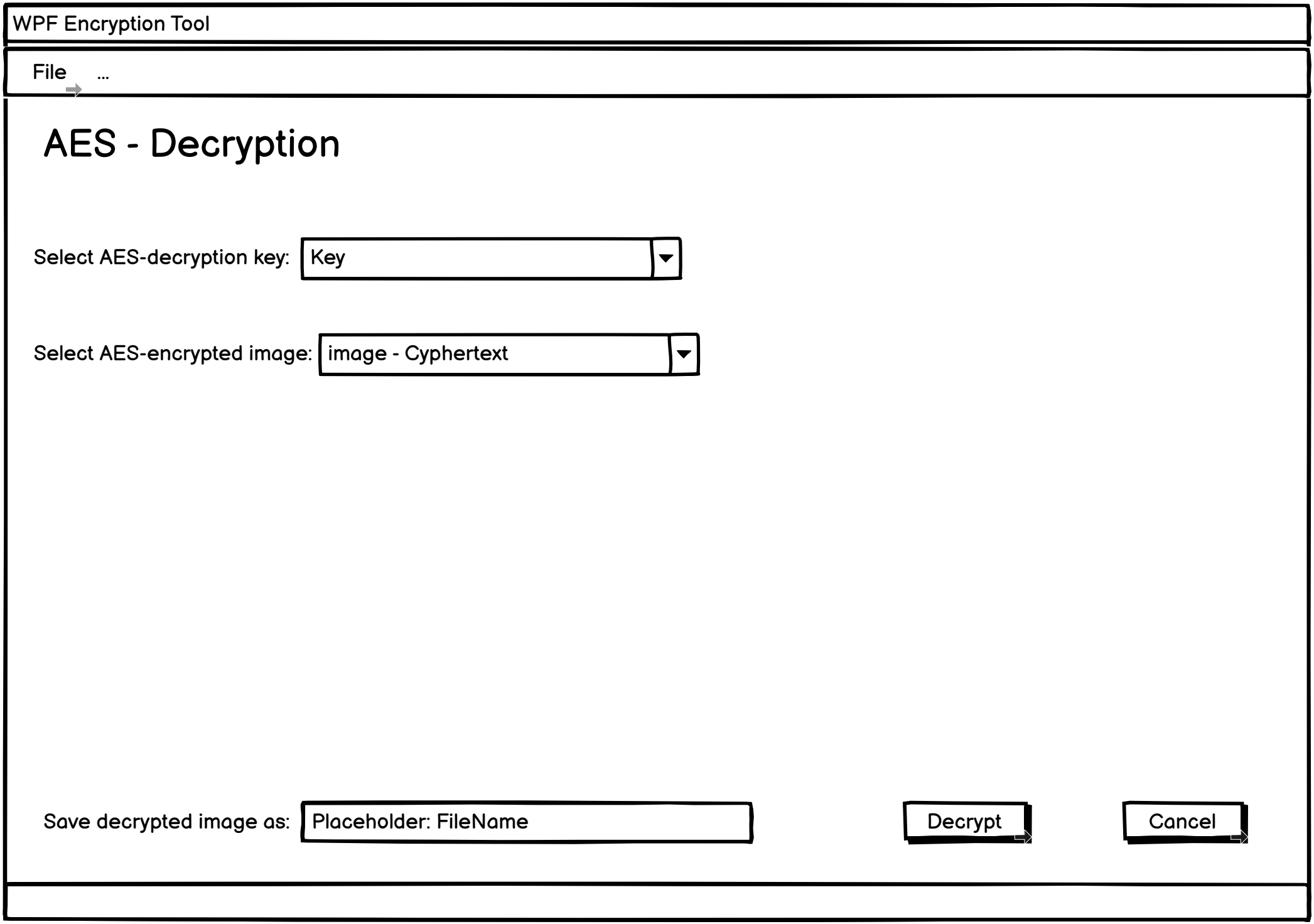
Select image: ... OnClick => OpenFileDialog

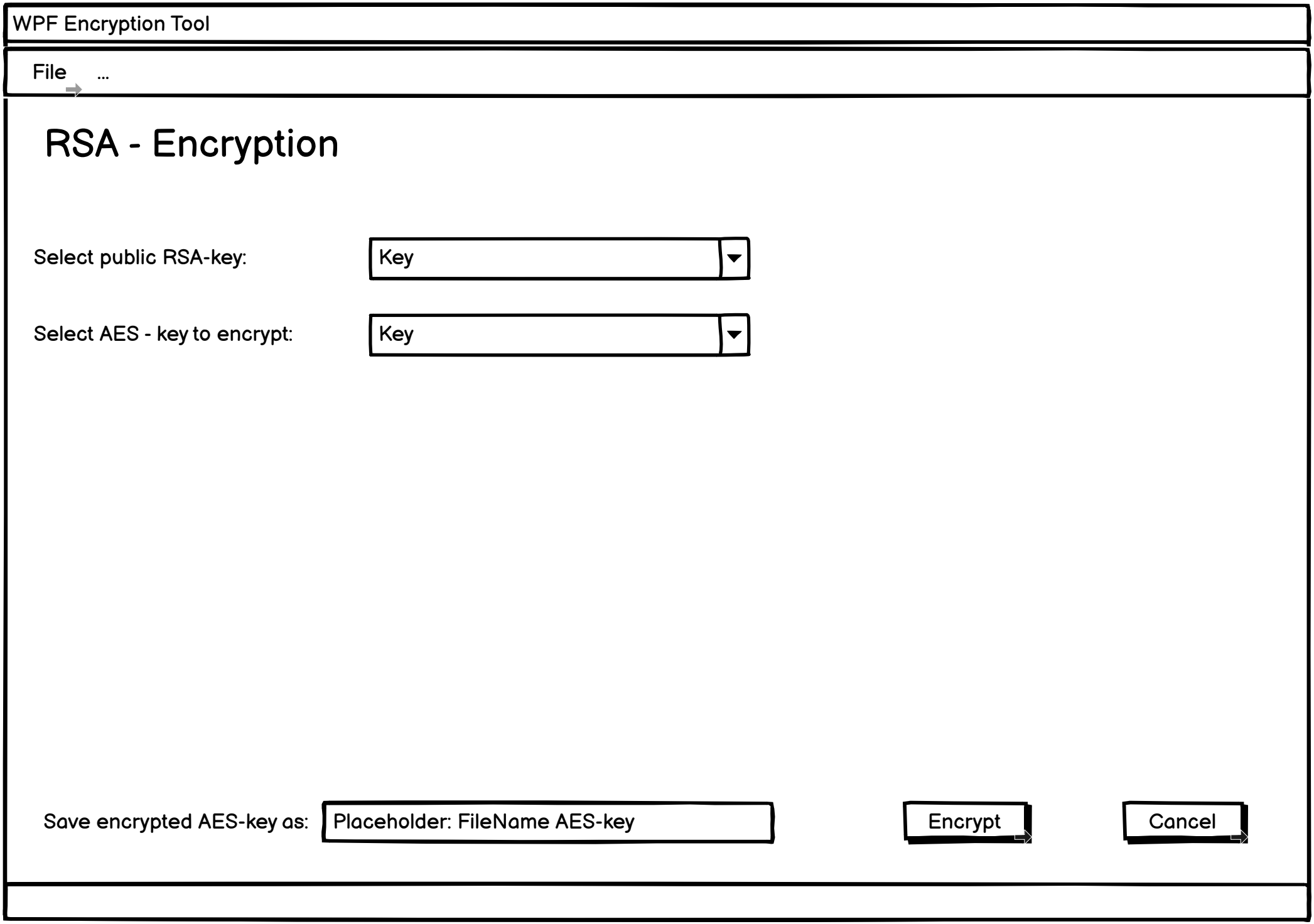
(Only *.bmp format is currently supported)



Save cyphertext as: Placeholder: Name cyphertext file

Encrypt Cancel


WPF Encryption Tool
File
...
AES - Decryption
Select AES-decryption key:
Key
Select AES-encrypted image:
image - Cyphertext
Save decrypted image as:
Placeholder: FileName
Decrypt
Cancel


WPF Encryption Tool
File
...
RSA - Encryption
Select public RSA-key:
Key
Select AES - key to encrypt:
Key
Save encrypted AES-key as:
Placeholder: FileName AES-key
Encrypt
Cancel

WPF Encryption Tool

File ...

RSA - Decryption

Select private RSA key: Key

Select AES - key to decrypt: Key

Save decrypted AES-key as: Placeholder: FileName AES-key

decrypt

Cancel