Author: rupp,scd
Project:secretforex
Date: 05/22/13

SECURE DOC READER USER'S GUIDE

Index

1. Introduction....1
2. Description....1
3. Personalisation....2
4. Shipping the book (alpha)....5
5. Reading the book from USB....8

Figures
Illustration Index

Illustration 1: selection of the script for launching the perso tool....2
Illustration 2: Flipbook directory (clear)....3
Illustration 3: secure doc perso GUI....4
Illustration 4: Ciphered flipbook....5
Illustration 5: Secure Doc Reader zip file....6
Illustration 6: Unzip secure reader in X:\....7
Illustration 7: USB sticker ready to be shipped....8
Illustration 8: Files deciphered by the secure Reader....9
Illustration 9: Using Secure Doc Reader....10

1. Introduction

This document describes how to personalize a flipbook for the secure doc reader and how to install the secure doc reader.

2. Description

The secure doc reader is a secure HTML engine that do not expose the source code or any of the resources of the source files that it is displaying.

The secure doc reader reads a DES or AES encrypted flipbook , internally decipher it and

read the decipher resources in a secret temporarily location.

WARNING:To use the reader, JAVA 7 must be used. The USB should include the installation of JAVA 7.

3. Personalisation

Unzip the two alpha zip files

Run the securedocperso tool by lauching either the batch file or the shell (linux) file.

This tool must not be shipped with the USB.

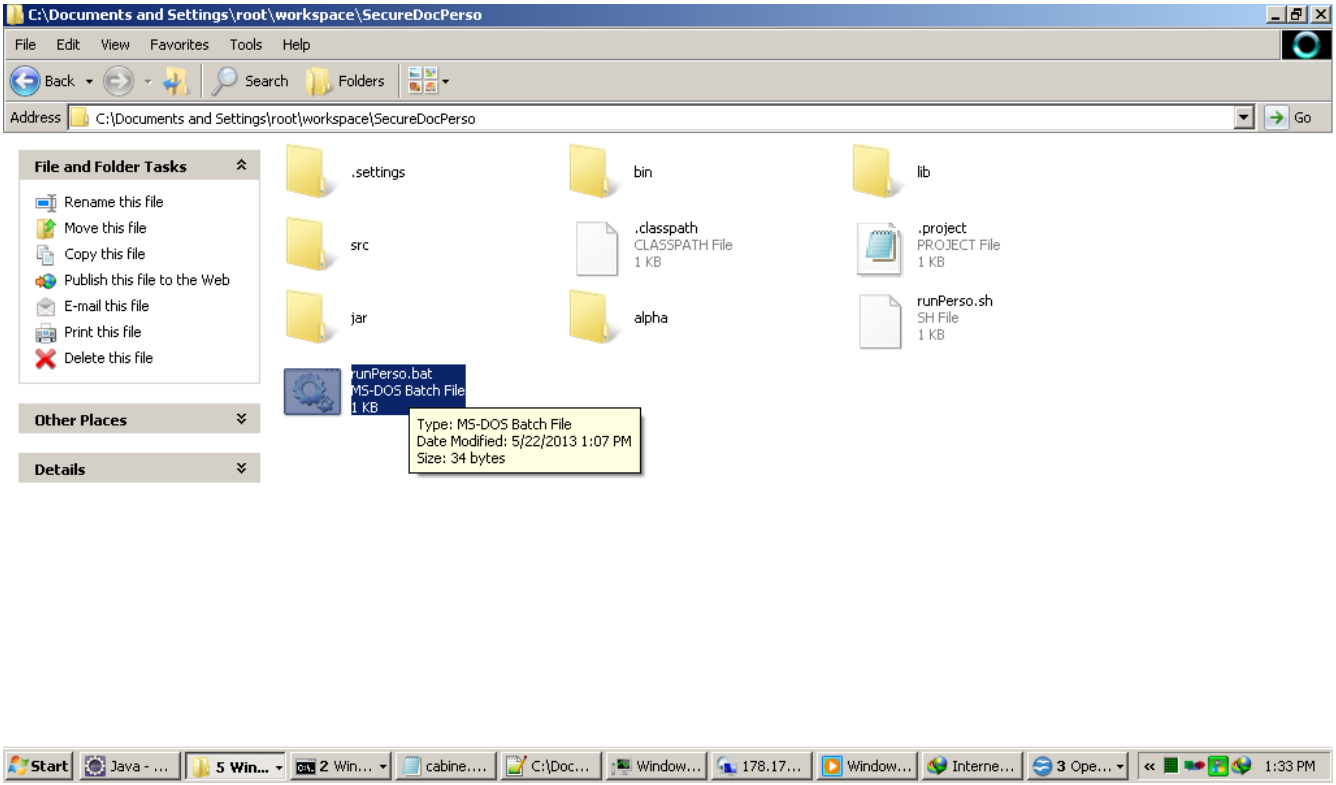


Illustration 1: selection of the script for launching the perso tool

This will launch the secure doc Perso GUI tool.

The key can be changed (in alpha version, the key must be left as it is)

The flipbook root directory must be specicified as the input files, here: C:\test_flipbook

The output directory for the ciphered files must be specified, this is the directory where the flipbook files with be ciphered anc copied. This directory will be shipped with the USB.

Choose any directory on your hard drive such as c:\test_flipbook_crypt for example.The directory do not need to exist (the perso tool will create it) but if it exists it must be empty.

Once the input and output directories have been chosen, it is only needed to run the encrypt button. After a few seconds, it will create the encrypted flipbook in the chosen output directory.

In alpha version,only DES is supported while in beta version, AES will be supported too.

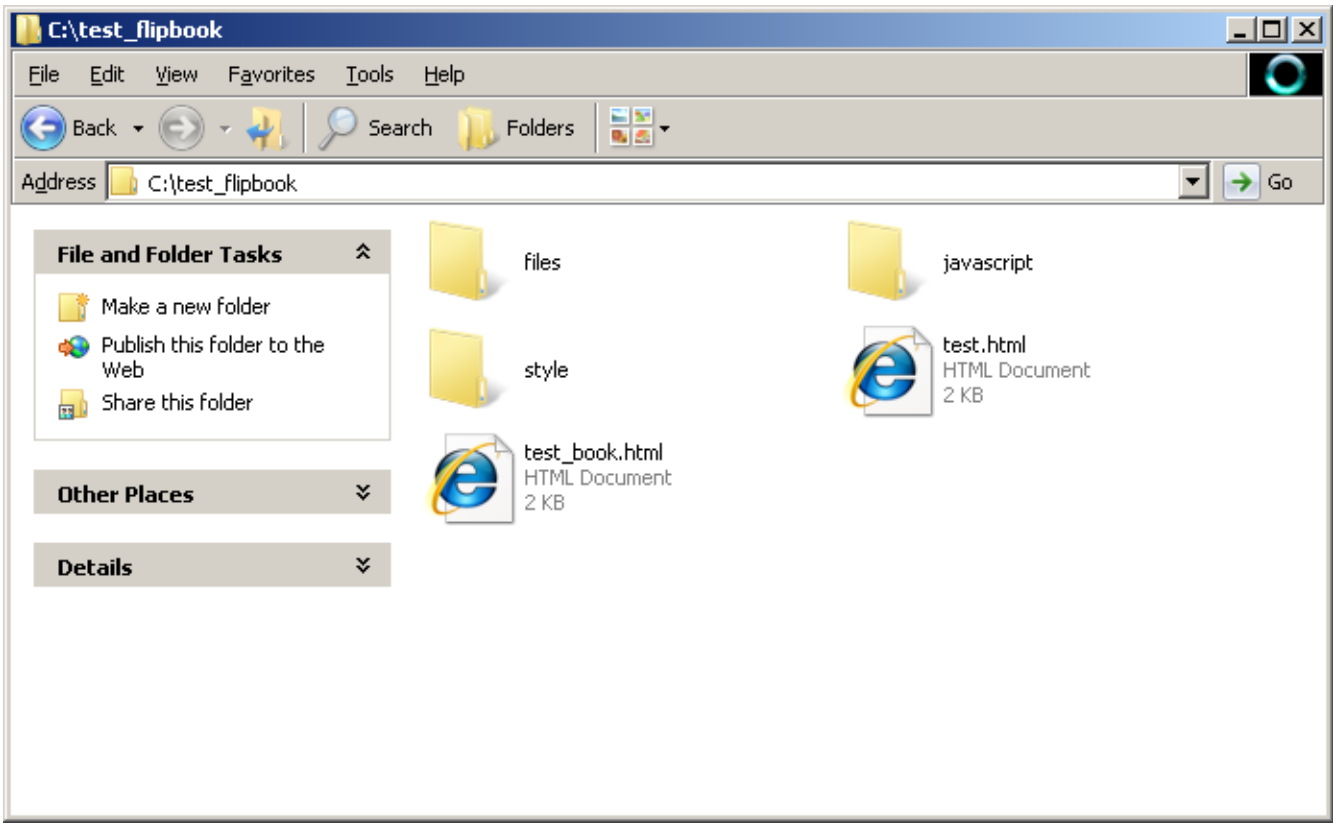


Illustration 2: Flipbook directory (clear)

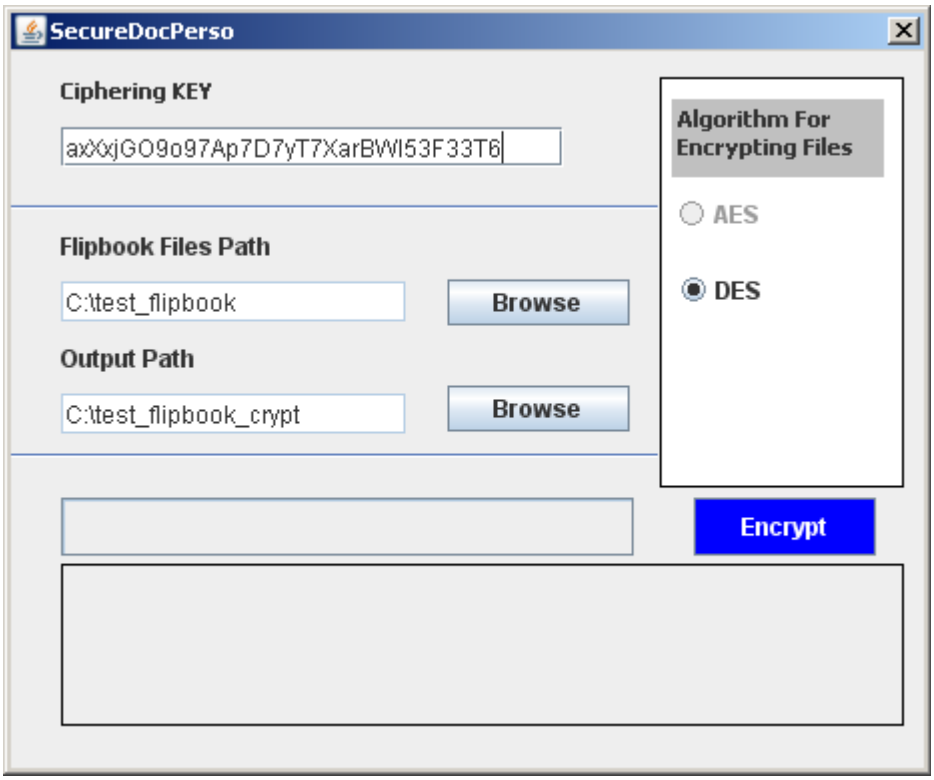


Illustration 3: secure doc perso GUI

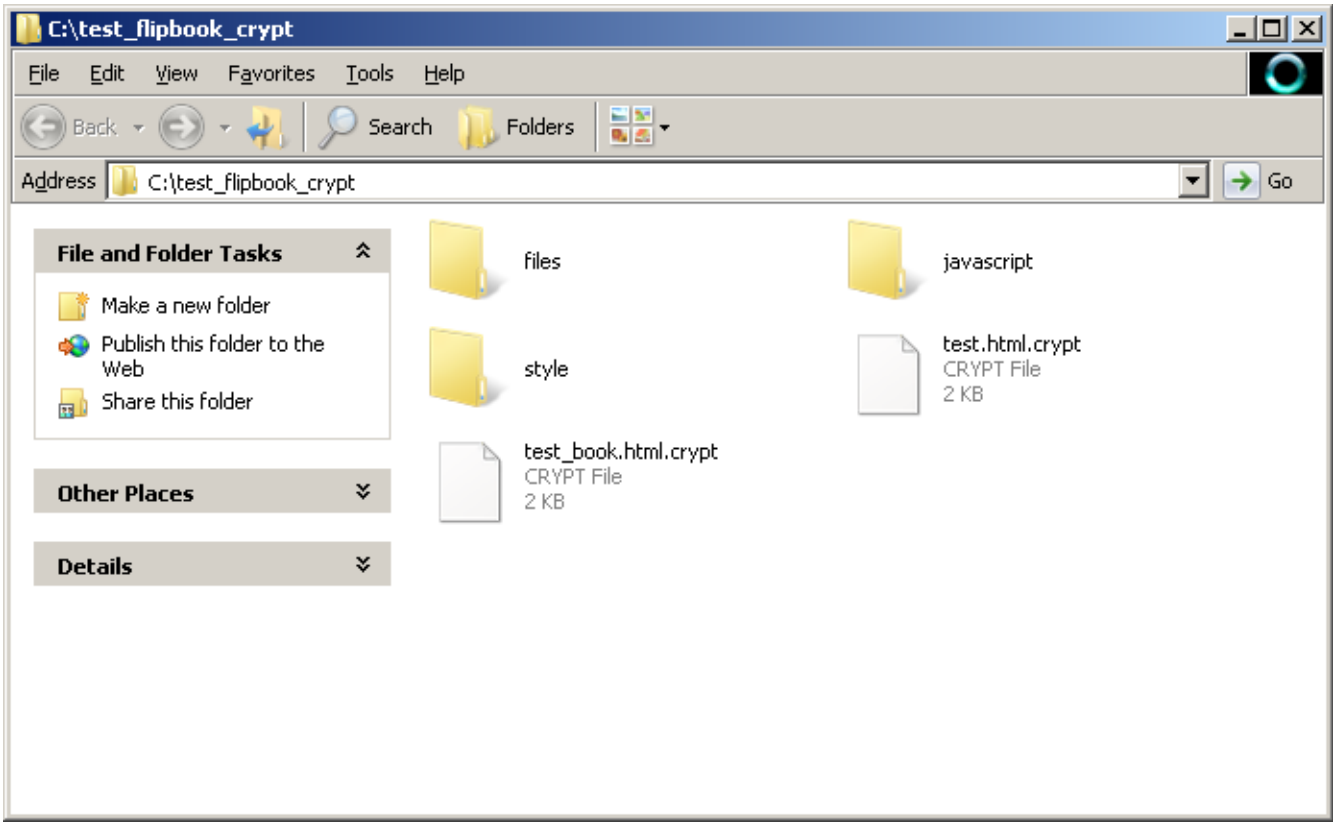


Illustration 4: Ciphered flipbook

4. Shipping the book (alpha)

In the USB sticker , say X:\, create a directory named flipbook, the content of the encrypted flipbook directory must be copied to X:\flipbook (note that X:\flipbook output directory can be directly specified in the perso tool)

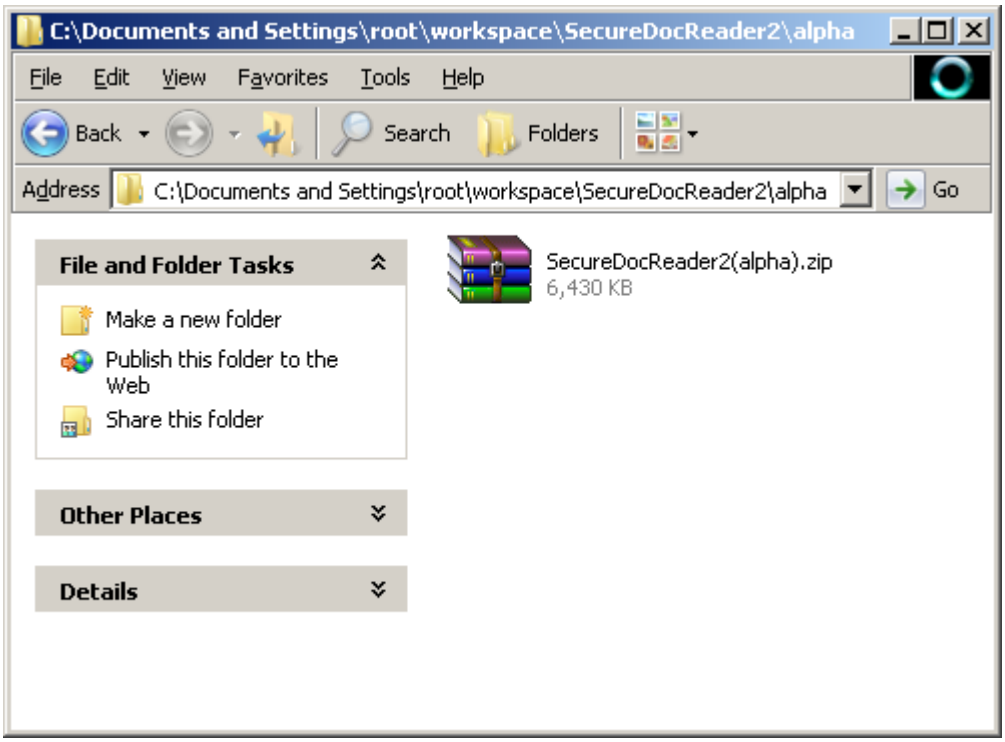


Illustration 5: Secure Doc Reader zip file

Unzip the secure reader in X:\ at the immediate root.

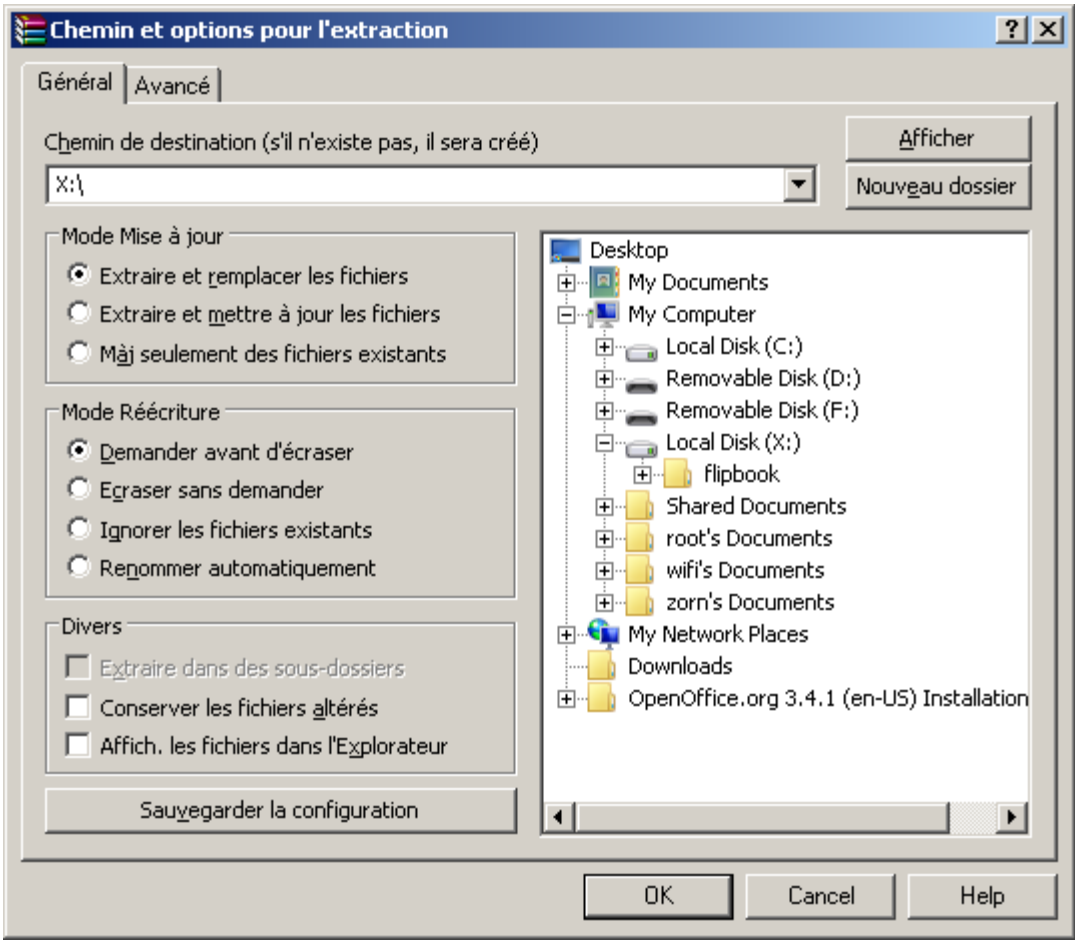


Illustration 6: Unzip secure reader in X:

The result must be the following:

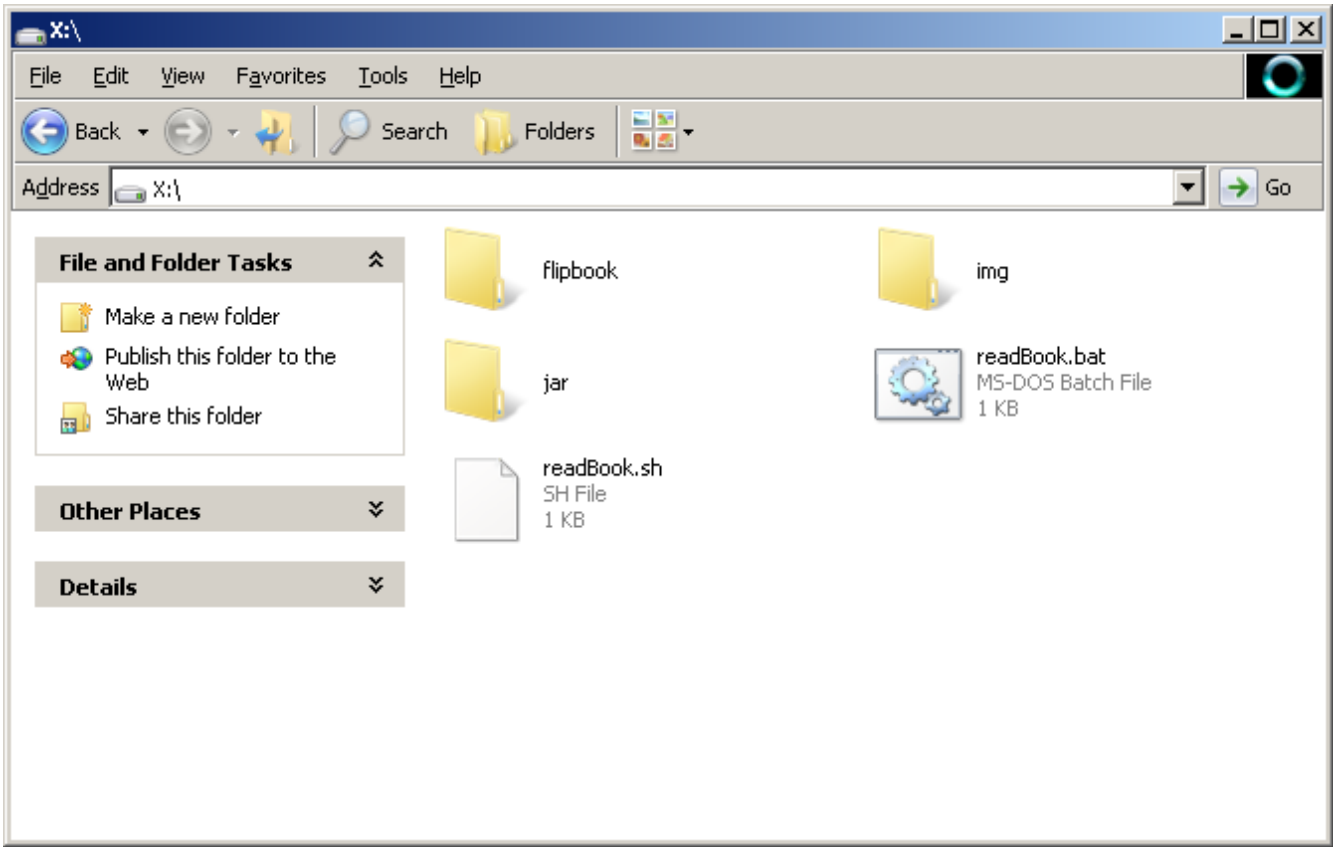
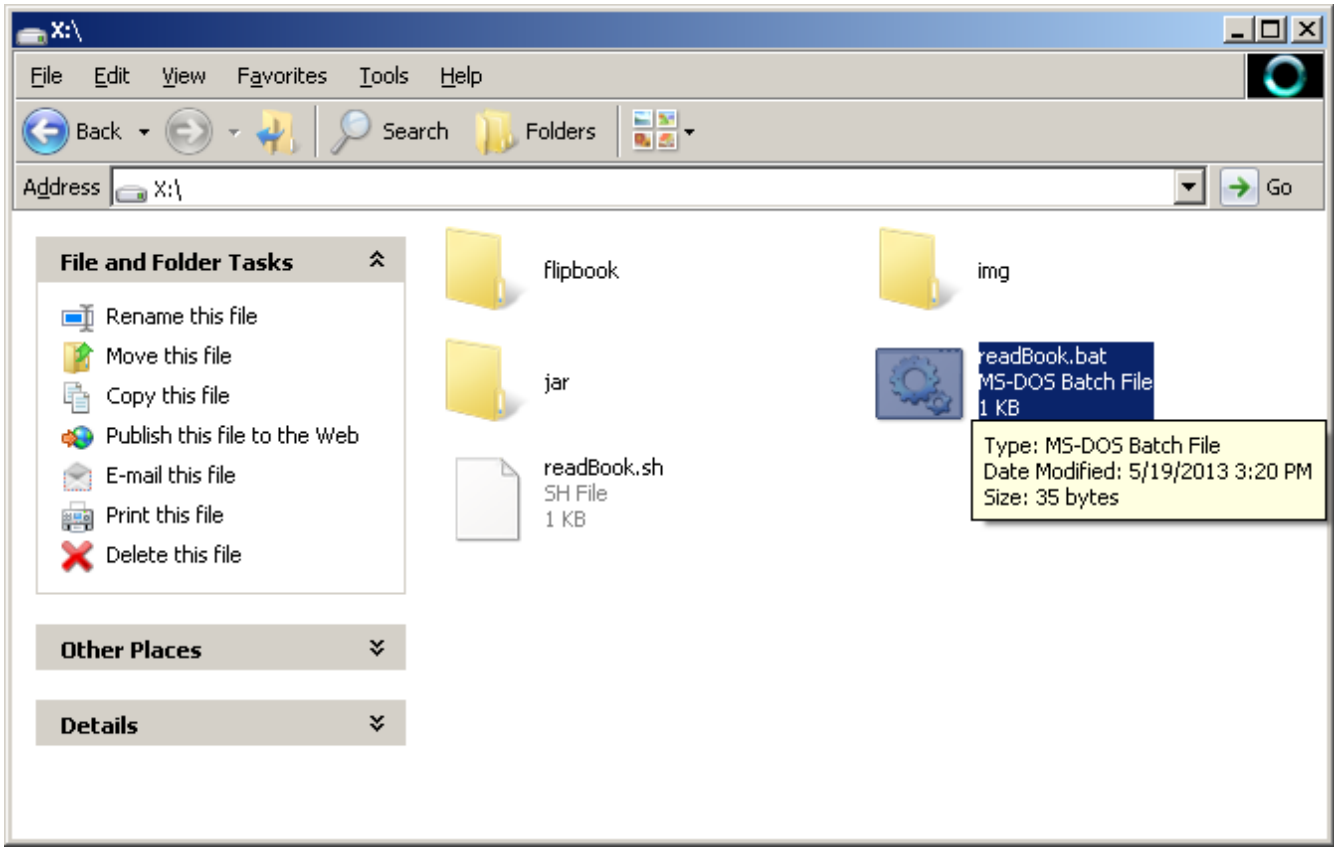


Illustration 7: USB sticker ready to be shipped

5. Reading the book from USB

Simply launch the bat or sh file:



The reader will start deciphering the files:

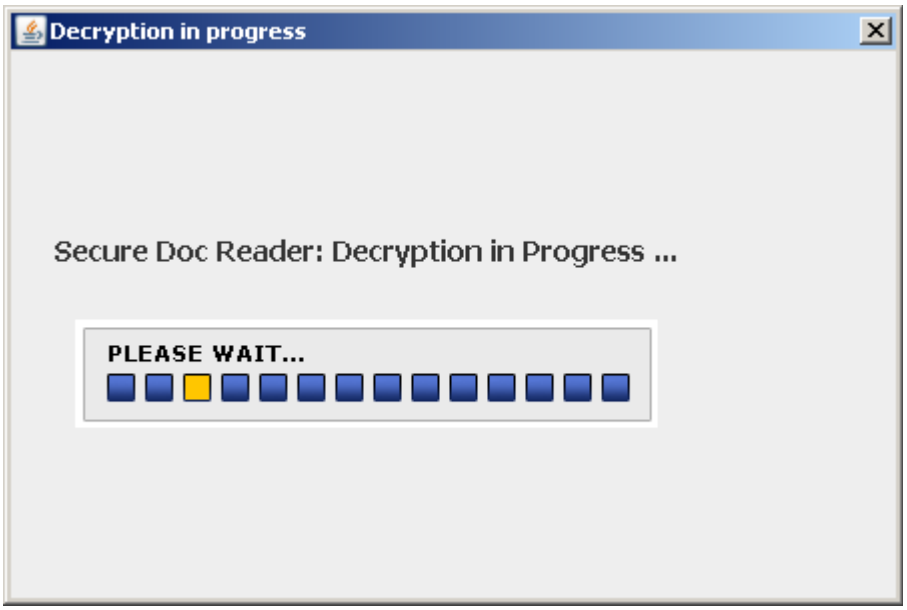


Illustration 8: Files deciphered by the secure Reader

The flipbook will be displayed in the java reader.

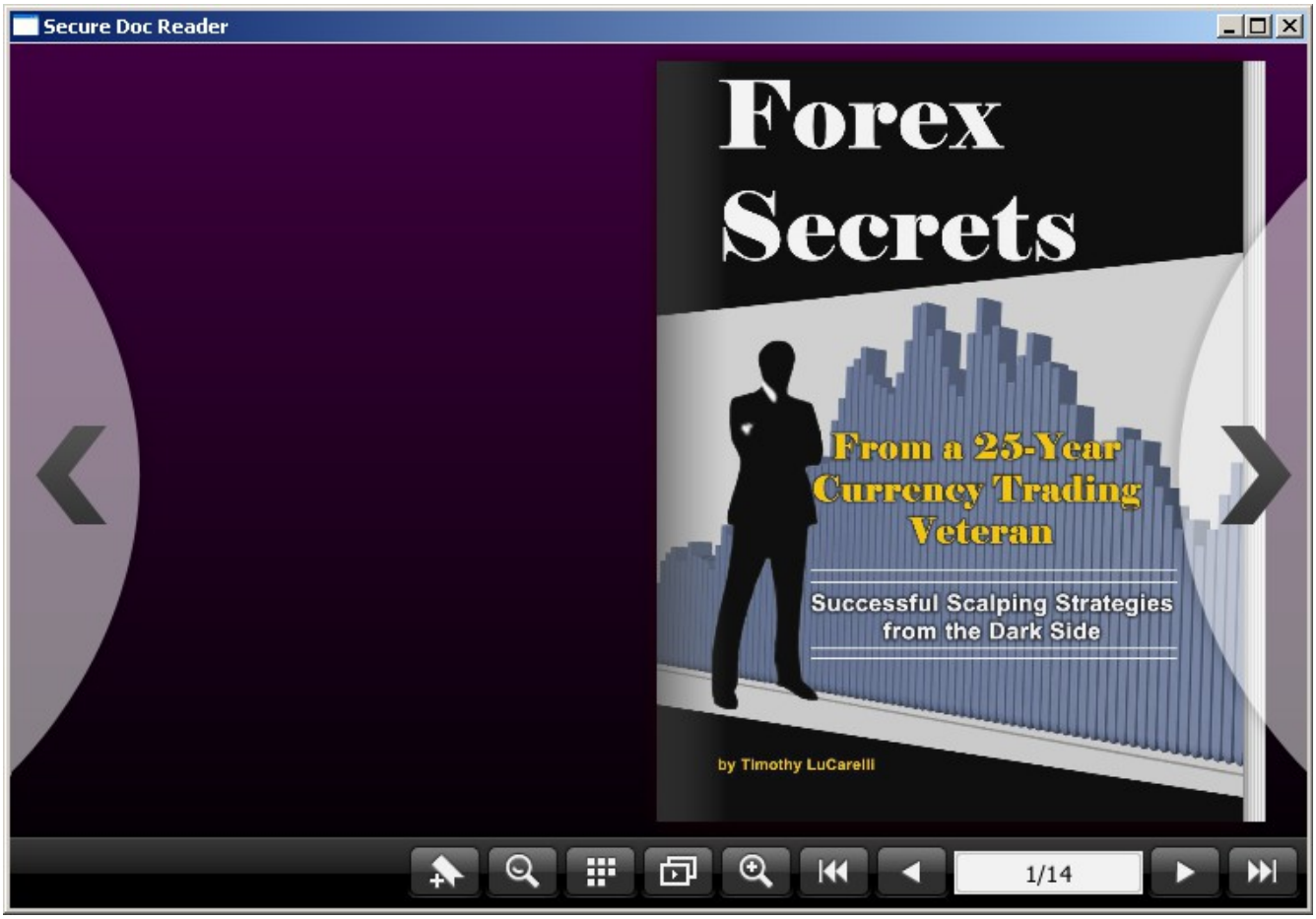


Illustration 9: Using Secure Doc Reader

The book is loaded using an HTML web engine but no interaction exists with the user except the flipbook navigation itself. The secure reader is completely locked. The source code of the HTML cannot be accessed and there is no way to save or access the HTML files displayed.The book can be used in full screen mode.

In the beta release the perso tool will directly ask for the USB stick letter, custom key could be used and AES will be offered as an alternative to DES. If needed , to improve the performance, a ram drive couold be created by the secure reader to load the files.

In beta version, the java code will be also obfuscated by the perso tool during the USB perso process.

The alpha version should be used to check performances and if there are some bugs