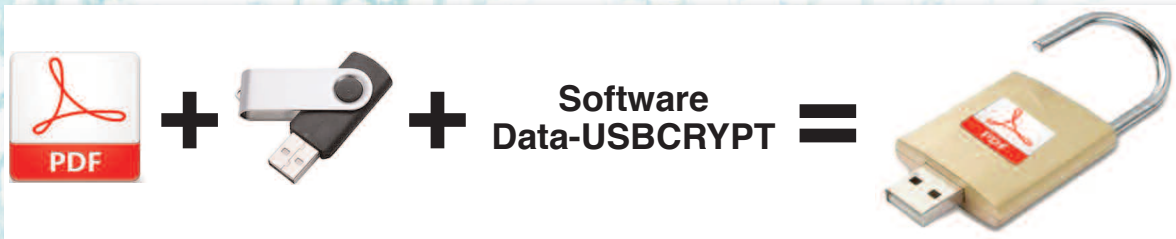


Data protection with encryption software and standard USB key ... Thanks to Data-USBCRYPT[©] software

State of the Art:

Today, there is no efficient solution to avoid PDF documents hacking.

What exists lets you define a password to protect your document. Unfortunately, nothing prevents the user to share or communicate this password, allowing unauthorized users to open documents. And so, to copy it, even if this document is encrypted.



Data-USBCRYPT software:

Data-USBCRYPT is a data protection based on files encryption with AES-128 protocol, associated to access protection through standard USB key. Using another key than the original, the file will stay encrypted and will be unreadable. This protection is physically linked to the original key with which you made the encryption.

This principle applies, currently, only to PDF files in which any content (text, image, multimedia) will be readable in a future version.

Advantages of this system are total security guaranteed by AES encryption and use of a standard USB key to work as a dongle. This plugged USB key will authorize opening PDF document. As you may have understood, you can, if you like, define an "optional" password in the PDF file and, in addition, encrypt it and use the USB key in order to decrypt, open and read your PDF file.

Compatible from Windows XP to Windows 8 (Windows 10 to be tested) and Macintosh from Mac OS X 10.7.

In case you lose the USB key with its content, the optional password that you defined will protect access to your documents. If you were hacked or if you made a backup of the encrypted content of the key, one will have to plug the USB key in the computer to be able to open an encrypted document.

As long as the key is plugged in an USB port of your Mac or PC computer, and provided that this is the original key, files may be decrypted and are readable and printable (optional), but may not be duplicated, nor saved, nor saved as... On the other hand, it is possible to duplicate encrypted documents.

Operation

A dedicated application "Editor", Mac and PC compatible, ensures the preliminary data processing: AES-128 encryption with your own secret code, gathering of all USB key parameters and creation of the access control file (unique and dedicated to the USB key that will contain data). So, you have to prepare USB key one by one.

There are two solutions for managing batches of large quantities of keys:

1) Manual solution

- Prepare encrypted data and copy it on all the keys (data is the same for all keys),
- Prepare key by key, at the time of sale, the access control file (unique and linked to one key).

2) Automatic solution

You have sold an USB key duplication system named DupliKey[®].

The software of this connected duplication system (Mac and PC compatible) is able to serialize USB keys as part of data protection. So, it's able to duplicate data and create the unique protection file for each key.

Planned enhancements:

Currently dedicated to PDF files, this Data protection via standard USB key will develop towards other document types, as Word, Excel, images, audio, video files and others. Don't hesitate to contact us if you want us to meet your needs.

Advantages:

- Use at a lower cost an hardware protection with a general public USB key (available in any computer shop),
- Total security for documents,
- Possibility of Internet deals: purchase of an additional document, book, updates, protected with the same USB key already owned by the customer, with the help of a database that you will manage.

Target:

Any company using or generating sensitive data which should not be copied. I.e.: banks, patents, secure data of states and, for a more general public, books editors, music editors, photos and videos editors.

This allows to give or lend original sources, knowing that the user will not be able to copy decrypted files while he/she has the USB key. Professional photographers and authors of digital information, you are the first ones concerned.

Pricing list:

Our product is sold depending on the keys quantity that you would like to protect. The **Data-USBCRYPT®** software is also available as a demo version. You would may use **Data-USBCRYPT®** to protect up to (VAT not included):

- 25 clés : 12,00 EURO
- 100 clés : 40,00 EURO
- 500 clés : 175,00 EURO
- 1000 clés : 300,00 EURO
- 2000 clés : 500,00 EURO
- 5000 clés : 1200,00 EURO

Our light demo version allows you to encrypt 3 documents or 3 folders containing PDF files and to link them with a unique USB key.

In the commercial version, we provide following options:

- Printing not permitted,
- Allowing printing from page XXX to page YYY,
- Printing page by page for the whole document, or only the current page,
- Authorisation for all printing according to PDF file authorisations,
- Opening the document with password,
- Authorisation for opening during X days from the first opening,
- Authorisation for opening until a certain date,
- Authorisation for opening from a date to another one,
- Authorisation for opening from a certain date,
- Authorisation for opening X times,

A lot of other options are still planned in future versions of our product:

- When wrong password entered more than X times, documents are deleted,
- Screenshots not allowed,
- Built-in Screen Saver, to hide screen after a certain inactivity delay, with optional password required to resume the job,
- ...