

# KeySec: A Look Inside

## General description

KeySec is a plug-in (additional module) for Adobe Acrobat 5.0, Adobe Acrobat Approval 5.0 and Adobe Acrobat Reader 5.0, which allows protecting a PDF document using the hardware keys “Smartkey”, produced by Eutron S.p.A.

In facts, KeySec allows encrypting a document in such a way that it can be displayed only when the key used to protect it is present in the system.



KeySec Reader is a limited version of KeySec, which only allows reading a document protected with KeySec (obviously, if you have a key valid for the document that you want to open).

## Characteristics of the Smartkey

A Smartkey is a hardware key for USB or parallel port. Each Smartkey has an IDCODE, i.e. an identification code, which is *not* univocal. This means that several Smartkeys with the same IDCODE can exist: as we will see later, this is especially important for KeySec. Each Smartkey, when produced, is given a serial number, which is unique for each physical key. Thus, a Smartkey has an internal memory with a certain size.

Smartkey is available in different models: the most indicated to be used with KeySec are the FX model, the PR model, the EP model and SP model. These models basically differ from other for the quantity of data that they can store: the FX model not equipped with memory, PR and EP models have a 64-Byte memory, while the SP model has a 416-Byte internal memory. Eutron suggests using at least the PR model.

The last characteristics of Smartkey are label and password: all Smartkey have an alphanumeric label, which allows their identification within the connection system and a password, alphanumeric as well, which should be entered to access the key memory. Since the FX model does not have a memory, it doesn't have a fixed password and label, while all the other models have a programmable label.

These are the ingredients used by KeySec: let's see how.

# Characteristics of KeySec

## ***Basic functions***

KeySec allows dividing PDF document users into three categories:

- The owner (unique) of the Smartkey used to protect the document
- The owners of Smartkeys authorised to open the document
- Those not included in the categories above

A set of rights can be granted to each category of users (right to print, right to modify a document, right to “copy & paste” the content, and so on ... ).

The owner of the Smartkey used to protect the document (called Master Key and identified by means of its serial number) has all rights on the documents, included the right to remove the protection and transform the encrypted PDF in a normal PDF, which can be displayed by everybody.

The owners of authorised Smartkeys are those with access to a Smartkey with the same IDCODE, same label and same password of the Smartkey used to protect the document.

All people without a valid key (or without any key) belong to the third category: generally, no right is granted to them, i.e. they can not even open the PDF.

Nevertheless, KeySec allows granting a set of rights to this category as well, even if Eutron advises against doing this for safety reasons.

In general, we can say that who doesn't own a valid key can benefit from certain rights (or, more often, no right at all), while who owns a valid key can benefit from more rights and , finally, who owns the Master Key can benefit from all rights.

## ***Advanced functions***

KeySec allows specifying a PDF expiration date when protecting the PDF itself. This date is stored in the document; when the document “expires”, it can be open only with the Master Key.

Furthermore, as we have already seen, a Smartkey can have an internal memory. If this is the case, KeySec allows specifying an expiration date for each physical Smartkey (i.e. for each serial number): the day after the specified expiration date, the Smartkey will no longer work. Key administrators, by means of a simple Web interface, control this setting; the date is materially written in the Smartkey when the product is activated.

## **Activation of the product (KeySec or KeySec Reader)**

A Smartkey dongle is supplied together with each copy of KeySec or KeySec Reader. Once the software installation is terminated, in order to use the product, it should be activated; you can activate the product in three ways:

- Via Internet on the same PC where KeySec or KeySec Reader have been installed
- Via Internet using another PC for connection
- Via Fax

The first two methods should be preferred, as they allow you to start using the software immediately. In simple words, you should connect with a normal Web browser to an Internet site; you will be prompted to enter an alphanumeric code (called personal code) generated by KeySec when requesting an activation. Based on this code, the site generates an activation code to be entered in the software in order to complete the procedure.

During these operations, the Smartkey to be initialised should be inserted.

The initialisation via fax mainly implies that the personal code is sent by fax to a defined fax number. The activation code will also be transmitted by fax.

To renew an expired key, the key user should follow a similar procedure, he should connect to a defined Web site to receive an updating code.

## **Example of step-by-step procedure for the distribution of a PDF document protected with KeySec**

In the following example we analyse two figures: the *operator*, in charge of PDF document protection and, by means of the Web interface, management of expiration date of keys distributed; and the *user*, who benefits from the documents protected by the operator.

The operator should have the following instruments available:

- Computer with Windows 98, 98SE, Me, NT 4.0, 2000 or XP
- Adobe® Acrobat® 5.0
- KeySec
- A Smartkey (that will become the Master Key of this distribution network)
- Connection to the Internet and Web browser

The user should have the following instruments available:

- A PC with Windows 98, 98SE, Me, NT 4.0, 2000 or XP
- Adobe® Acrobat® 5.0 or Adobe Acrobat Approval 5.0 or Adobe Acrobat Reader 5.0
- KeySec or KeySec Reader
- A Smartkey supplied by the operator (therefore, with the same IDCODE of operator's Master Key)

Procedure for the operator:

1. Open Adobe Acrobat 5.0

2. Activate KeySec connecting to the special Web site (only for first use)
3. In Acrobat, open the PDF you want to protect
4. Insert the Smartkey (Master Key) in the USB or parallel port
5. Select the menu control in Acrobat that allows applying a protection to a PDF document
6. Establish a label and a password for the Master Key of this distribution network and set them
7. Select the rights granted to authorised key owners (i.e., with the same IDCODE, same label and same password of the Master Key)
8. Save the document, which now is encrypted and protected
9. Connect to the Web site for your own key management and set the expiration date and password of each key. The password should be identical to the one used for the Master Key
10. Distribute protected PDF and Smartkey to users, transmitting the Master Key label to users.

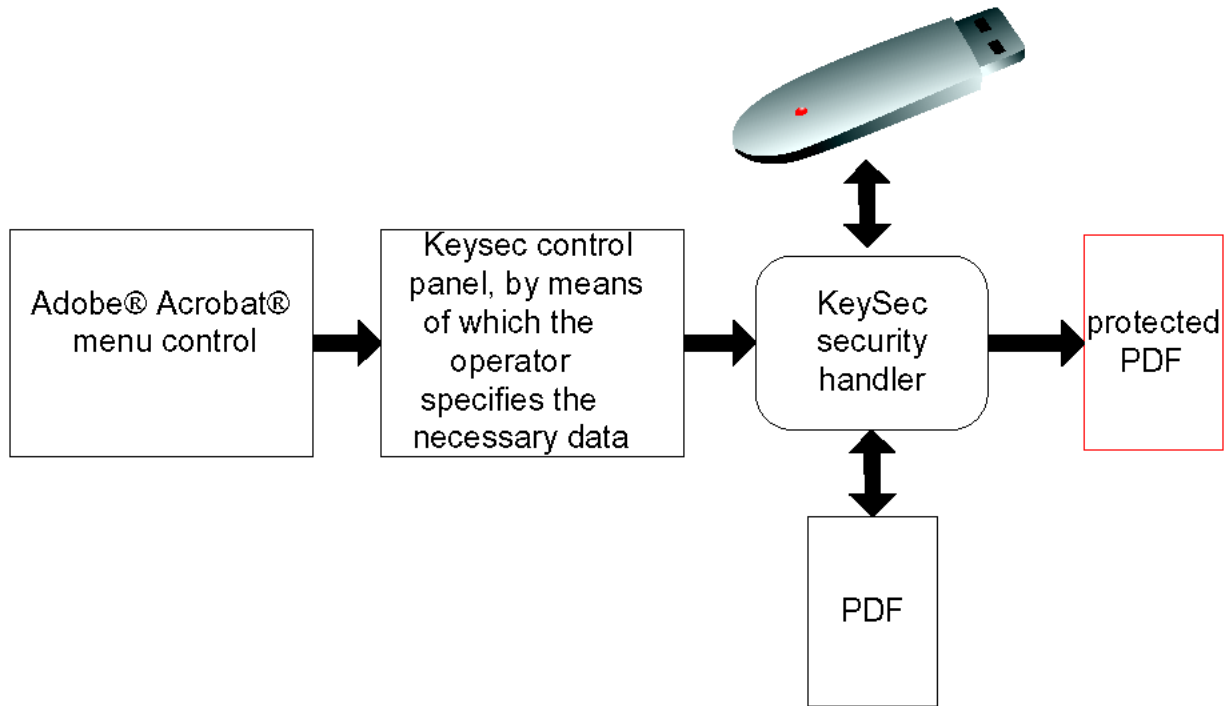
The steps 3 to 8 can be carried out in batch, i.e., automatically on a large quantity of documents.

Procedure for the user:

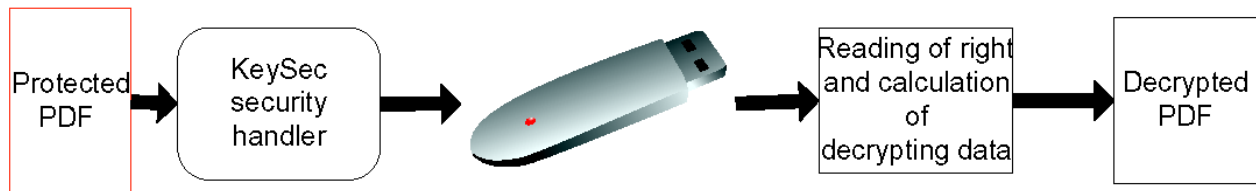
1. Insert the Smartkey received from the operator in the USB or parallel port
2. Open Adobe Acrobat 5.0 or Adobe Acrobat Approval 5.0 or Adobe Acrobat Reader 5.0
3. Set the label transmitted by the operator (only for first use)
4. Activate KeySec or KeySec Reader by connecting to the Web site indicated (only for first use)
5. Open the document

In order to complete points 3 and 4, the user should be aware of the label set by the operator for the Smartkey of this distribution network. On the contrary, the password will be transmitted to the software by means of the activation code, thus ensuring the safety of data stored in the key memory.

## CREATING A PROTECTED PDF



## OPENING A PROTECTED PDF WITH AUTHORISED KEY



# DISTRIBUTION DIAGRAM

