

WINDOWS

Aloaha PDF Crypter



Aloaha PDF Crypter

© 2010 Wrocklage Intermedia GmbH

Aloaha PDF Crypter

© 2010 Wrocklage Intermedia GmbH

All rights reserved. No parts of this work may be reproduced in any form or by any means - graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems - without the written permission of the publisher.

Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners. The publisher and the author make no claim to these trademarks.

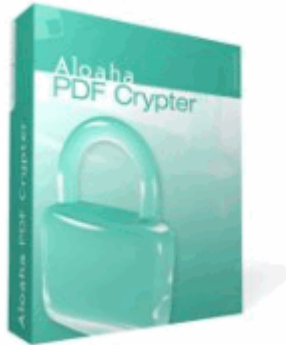
While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

Printed: Januar 2010

Table of Contents

	Page
1. Introduction	4
2. Installation	5
3. Usage	8
3.1. Functionality of the Aloaha PDF Crypter	13
4. Security	14
5. Personal search	15
6. Digital certificates	16
7. Application examples	17
8. PDFCrypter Hotfolder	18
9. Aloaha Key Finder	19
10. FAQ	20
Index	22

1. Introduction



Aloaha PDF Crypter Feature List

- PDF Encryption PDF 1.5 compatible (Reader 6)
- Certificate based Encryption (X.509)
- multiple certificates supported
- Only owner of private key can open document
- No Passwords needed
- Multiple owners possible
 - A list of certificates/authorized people can be defined to be allowed to open encrypted PDF.
- OCX Component included
- Can replace old traditional security (APDFPR)
 - (traditional password based security is extremely insecure! For example lost passwords can be removed with the Aloaha PDF Editor)
- S/MIME Mailer included
 - This intelligent mailer will send your PDF in an encrypted S/Mime email which is automatically signed with your certificate!
- can be assigned to right mouse click in windows explorer
- Drag&Drop supported
- PDF Attachments
 - One underrated feature of PDF is its ability to act as a container for other files. One example of where this could be useful would be attaching the original Word, Excel or other source files to the final PDF document, allowing it to be more readily updated. Since it is possible to attach literally any type of file, the PDF can also act as a secure delivery medium for sensitive or commercial content. You can just drag and drop your files to be attached on the "Files to embed" screen and Aloaha will embed them into your PDF before encrypting.
- Encryption API (Enterprise Version only)
- NO Adobe Software needed!

Freeware Features

- Non PDF Files can be encrypted/decrypted
- S/MIME Mailer
- re-distribution of installation package allowed
- Usage of OCX/ActiveX in other applications allowed

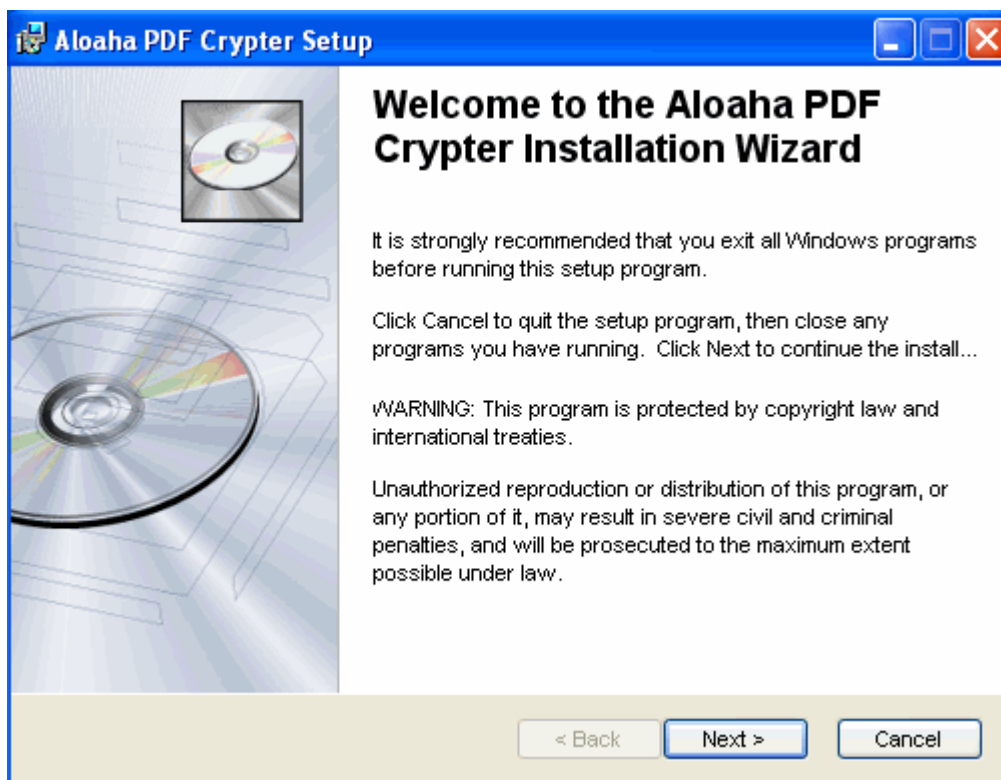
The Aloaha PDF Crypter encrypts your PDF files on the basis of receipt certificates. Only authorised recipients can read or open the file.

2. Installation

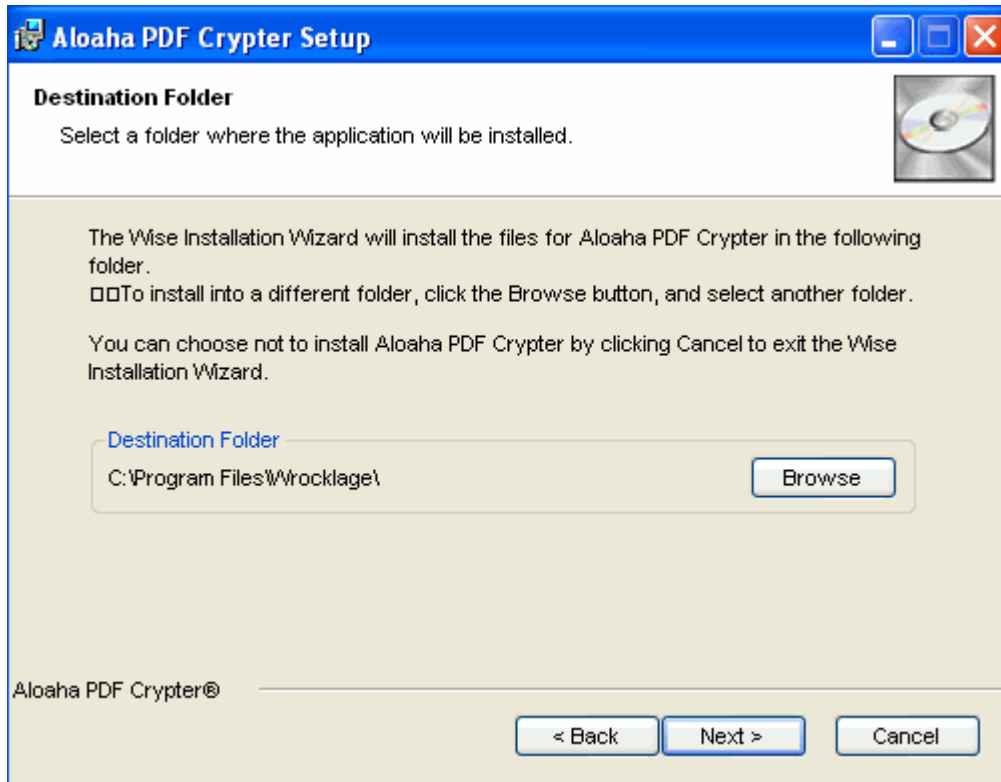
To install **Aloaha PDF Crypter**, start the installation file. (*aloaha_crypter_setup.exe*).



After the language is chosen, the following dialogue opens.



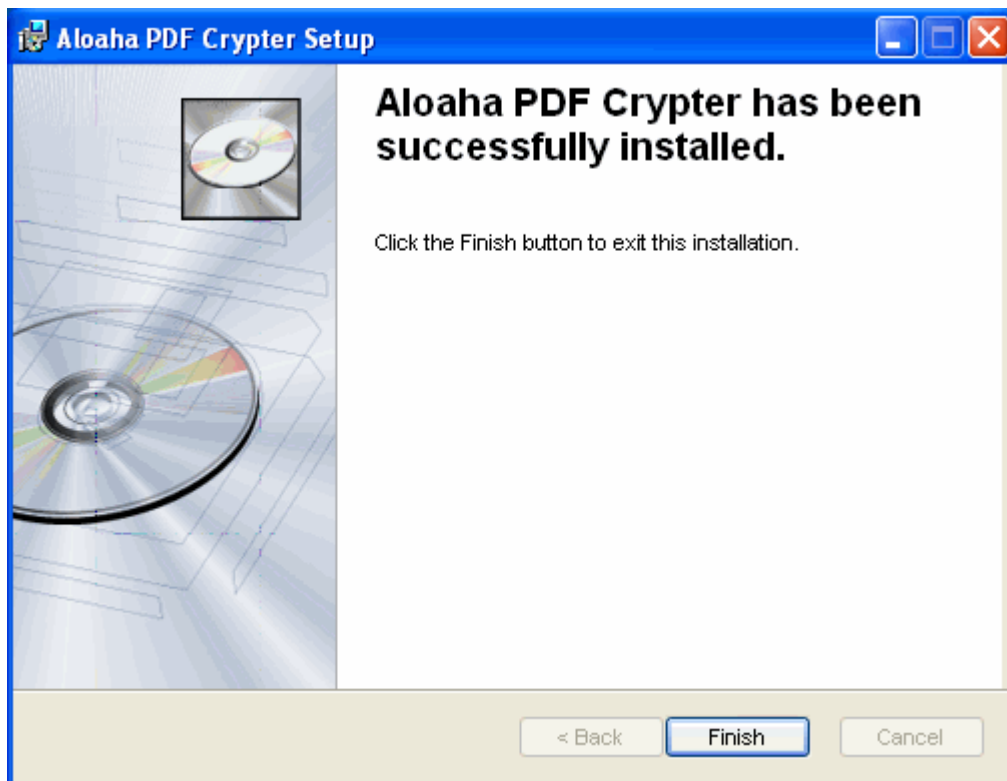
Setup will ask you for the installation folder before it begins to install the product. For installing in a different folder, click the Browse button, and select the folder you want to install to.



To use the given destination folder, confirm the selection with "Next" so that the installation routine can be launched. Select if necessary a divergent directory. Click moreover on "search".

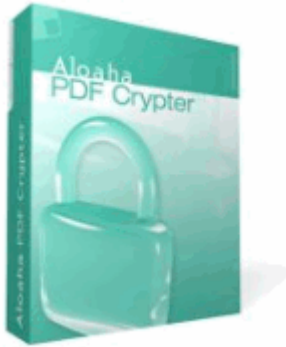
Note: The standard-installation path can mostly be accepted.

The following window informs about the advance of the installation process. If you click on "cancel", the installation process is exited and the already in the system saved data will be deleted.



If setup has installed successful the application you have to click the finish button.

3. Usage



Encrypt your PDF files with certificates

Aloaha PDF Crypter - Encrypt PDF files

With the Aloaha PDF Crypter you are able to encrypt your PDF files with receiver certificates.

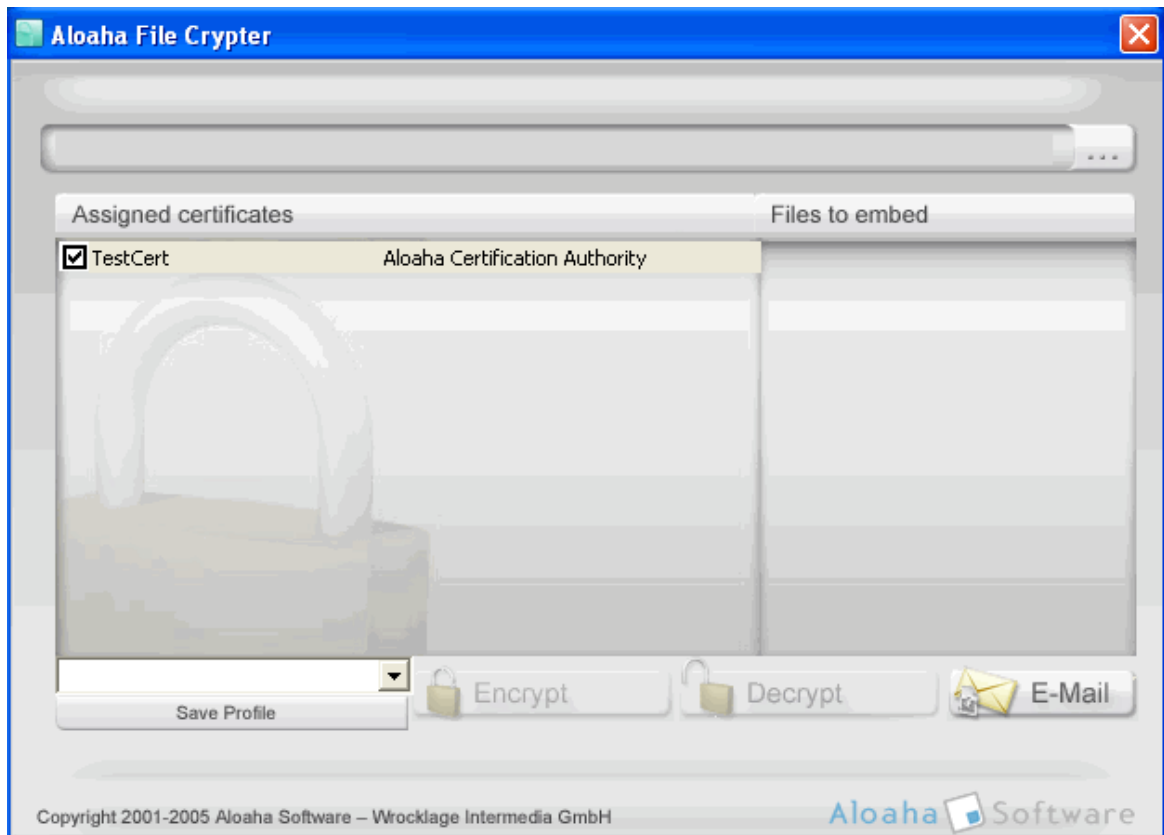
Open a file, select the receiver and click on "encrypt". Now the file is encrypted and can be opened only by the receiver.

Finally you can dispatch your contracts, accountancy documents and other confidential documents without everybody can open them.

The Aloaha PDF Crypter does not work with a password but with certificates. Thus is excluded that the file can be "cracked" by trying out code-words.

To launch Aloaha PDF Crypter, select the program Aloaha PDF Crypter in Windows start menu as shown below:

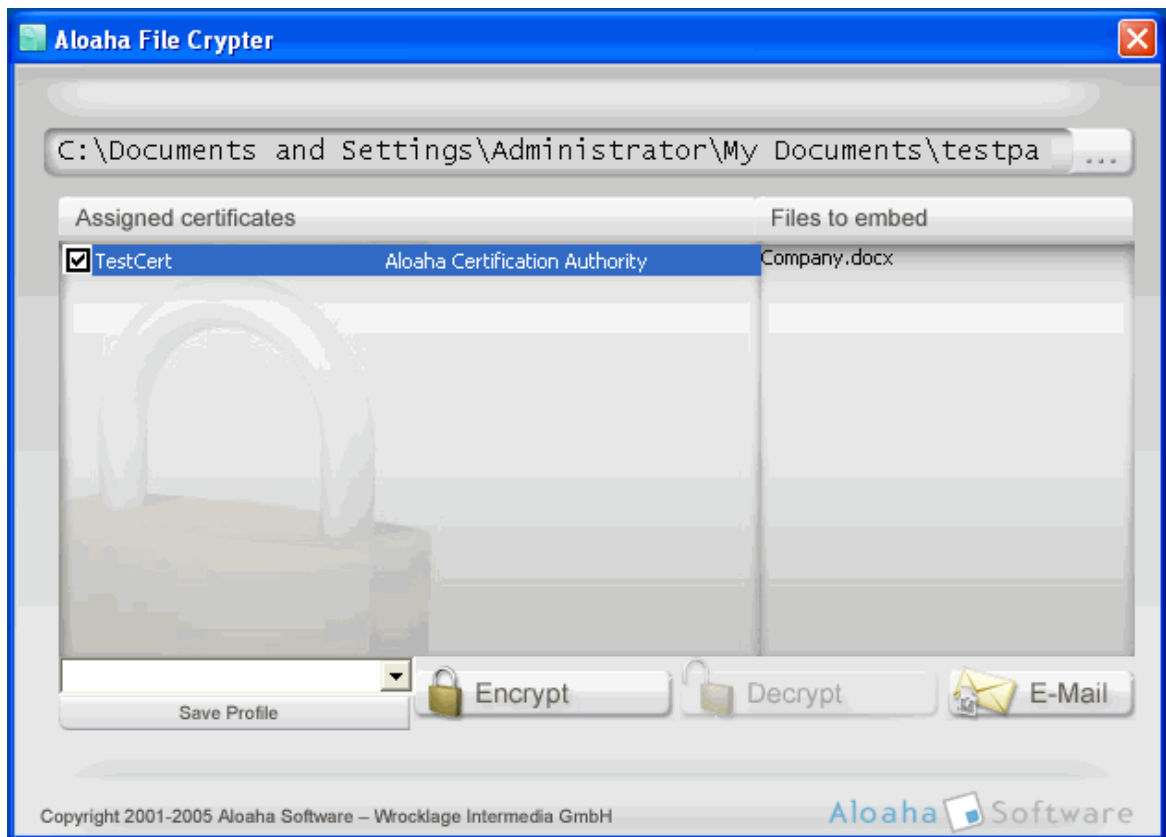
Start>All Programs>Aloaha>Aloaha PDF Crypter



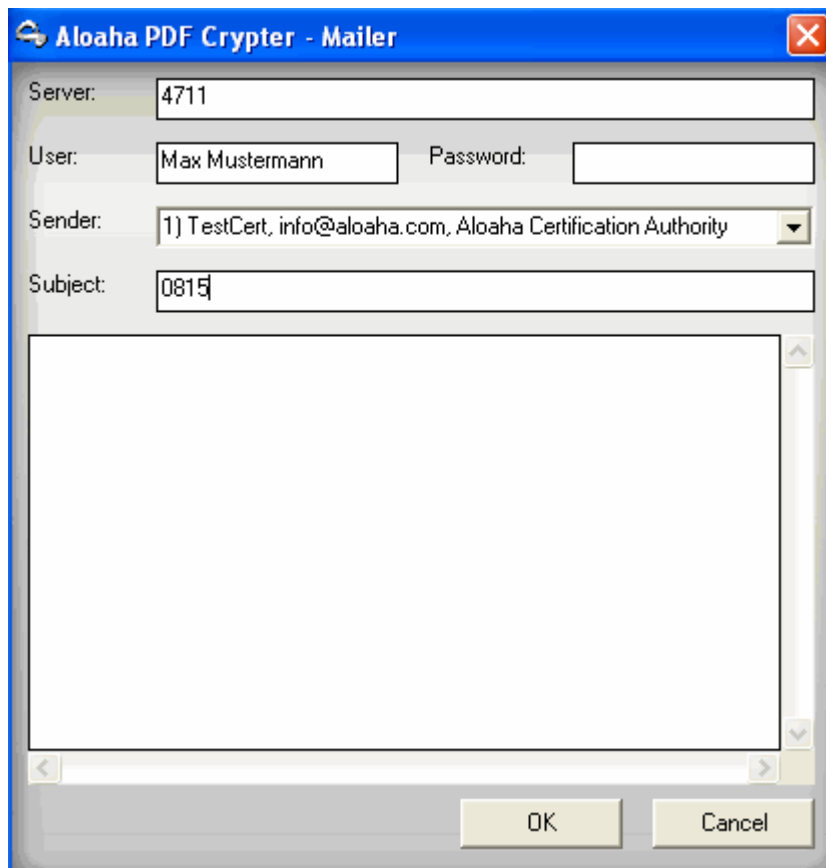
With the Aloaha PDF Crypter you can decrypt or encrypt PDF files and send decrypted or encrypted files by e-mail.

Choose the requested document which should be encrypted with "Browse".

Afterwards you select the certificate which should be assigned. With a click on "encrypt" the suitable certificate will be assigned to the document.



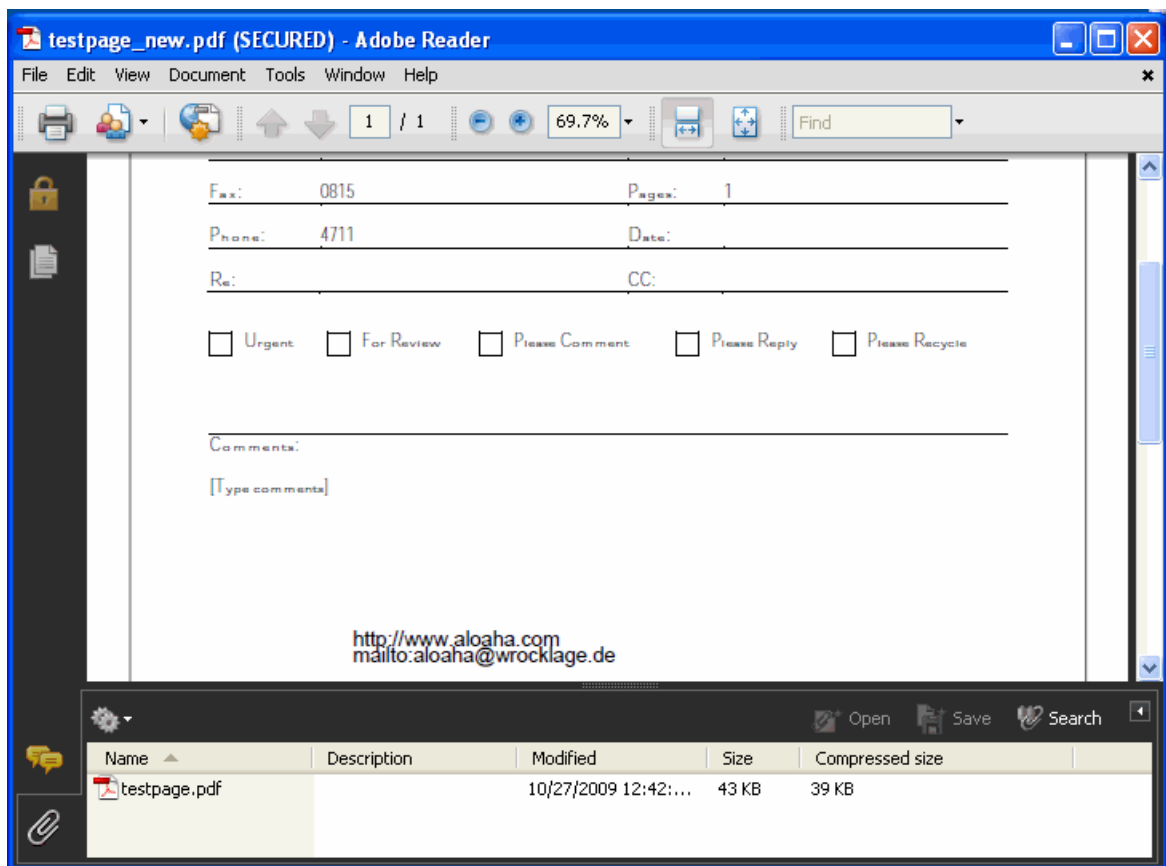
After you have encrypted or decrypted the document, you can send it when required by e-mail. Click on "e-mail", afterwards the **PDF Crypter Mailer** opens.



The screenshot shows a dialog box titled "Aloaha PDF Crypter - Mailer". It contains the following fields and controls:

- Server:** Text input field containing "4711".
- User:** Text input field containing "Max Mustermann".
- Password:** Text input field (empty).
- Sender:** Dropdown menu with the selected option "1) TestCert, info@aloaha.com, Aloaha Certification Authority".
- Subject:** Text input field containing "0815".
- A large empty text area for the email body.
- OK** and **Cancel** buttons at the bottom.

You are also able to embed files in the PDF which are encrypted with the PDF document. If you now open the PDF document with the Adobe Reader you will see the embedded file as an attachment.



3.1 Functionality of the Aloaha PDF Crypter

Background of the program

What happens while encrypting with the Aloaha PDF Crypter?

The PDF document is encrypted with the public Keys of the chosen receivers.

How does the Aloaha PDF Crypter work?

Select the certificates on the left. Then you drag the PDF document and click on encrypt. You can also add certificates while you shift them by Drag and Drop in the certificate list. On the right side (Files to embed) you can add files by Drag and drop. These are inserted before encrypting as an attachment in the PDF document.

How does the cryptographic encrypting operate?

You encrypt with the public Key and therefore the PDF document can only be opened by the owner of the private Key.

4. Security

Security by digital certificates

Security is reached by use of the public key of your electronic signature. The receiver or the receivers can read the PDF file by means of Adobe Reader from version 6. In opposition to password-protected PDF files the certificate security cannot be avoided with add-in programs.

Security in PDF files

PDF files are compatibly encrypted with Adobe Reader 6 and Adobe Reader 7. The receiver needs no additional software around the document.

Security in non-PDF files

Non-PDF files are saved as Aloaha files. Before saving as Aloaha files they were encrypted and compressed. To decrypt these files the Aloaha PDF Crypter is necessary. The encryption / decryption functions for non-PDF files are free functions. Therefore is no licence necessary.
Die Ver- und Entschlüsselungsfunktionen für Nicht-PDF-Dateien sind freie Funktionen, wofür keine Lizenz erforderlich ist.

5. Personal search

Sometimes it is necessary to dispatch an encoded document to people whose public Key and / or e-mail address is not known. Unfortunately, there is no data bank, as for example a phone book to search according to this information.

Publicly Keys can be found via LDAP in the PKI (Public Key Infrastructure) which is used by the receiver. If you do not know the PKI of the receiver use the Aloaha Key finder!
The Aloaha Key finder uses an easy text file which contains a list of the most popular PKIs and browses for the public Key of the receiver.

Windows search for people

Every modern Windows version has integrated the function "search for people". To search for people you open the **Windows top menu > search > people or computers**

If the searched person is found, the public Key can be accessed. It can be exported in the table of the digital IDs.

From a general table you can add the person to your address table by which the Aloaha PDF Crypter allows the access to the public Key.

6. Digital certificates

Digital certificates or digital signatures are used to identify persons on computers and in the Internet correctly.

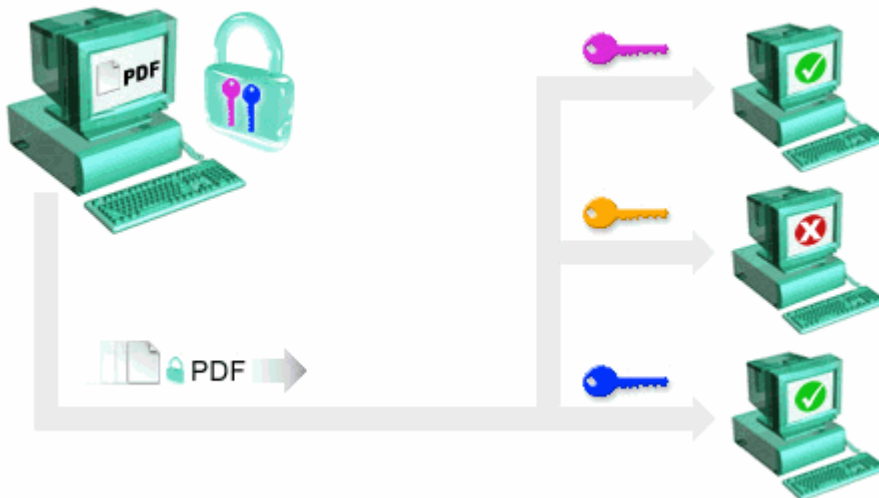
Certificates are published by certification authorities. A certificate always exists of two parts, the private key and the matching public key. The public key is administered by the certification authority (trust centre) and is published in a directory.

If a document was signed digitally, the receiver can check the genuineness of the encrypted document with the help of the public and the private key.

Certificates are offered in different security steps which are divided into following classes:

- Class 0 certificates are ordinarily test certificates without juridical background.
- Class 1 certificates confirm the genuineness of an e-mail address.
- Class 2 certificates confirm the genuineness of an organisation or a company. These certificates are intended primarily for the saved communication between already known partners.
- Class 3 certificates are the safest certificates and contain a personal identity check of the person. Besides, the person is identified with the help of a valid identity card and the certification authority makes sure that the civil status contained in the certificate with the entries agrees in the identity card.

After checking by the certification authority the key pair is delivered to the user (e.g., on a card with electronic chip by post) and the certificate published. Then every document can be signed with the suitable software digitally.



7. Application examples

Aloaha PDF Crypter is ideal for everybody who must administer confidential documents. Only the receivers can open the files. This is, e.g., for:

Banks (bank statements, etc.)
Lawyers (contracts, draught contracts)
Accountancy (balances)
Field service (confidential company information)

Briefly, for all informations, e.g., by e-mail to receiver beyond the company should be readable, extremely interesting.

8. PDFCrypter Hotfolder

In enterprise environments it might be necessary to automate the PDF Encryption process. Online Bookstores can integrate Aloaha PDF Crypter via the Crypter API in their .NET, ASP or PHP Webshop. The Aloaha PDF Crypter API is only available in the Enterprise Edition.

Much more popular than the Aloaha Crypto API are the Aloaha Crypter hot folder. The Aloaha PDFCrypter watched folder allow defining a folder to encrypt any PDF document dropped into that folder with the public keys configured. The dropfolder functionality is available in the Server Edition.

The Aloaha Crypto Folders are the ideal way to encrypt your PDF documents before moving them to the pickup folder of your document management system.

Configuration of Aloaha PDF Crypter Hotfolder

To be able to use a hotfolder a mechanism is needed to monitor these folders. To keep the configuration simple Aloaha PDF Crypter will utilize the hotfolder mechanism of the Aloaha PDF Suite. Please install the Aloaha PDF Suite from http://www.aloaha.com/download/aloaha_pdf.zip

The next step would be to activate the PDF Suite service. First right click on the Aloaha systray icon and exit Aloaha. Please open the services control panel and configure the PDF Suite service to startup automatic. Furthermore you need to remove the Aloaha shortcut from the autostart/startup group of the Windows Menu. Start the PDF Suite service and check with a right click on the Aloaha tray icon that interactive is not enabled!

Now you are ready to configure the hot folder. Please follow the steps below to configure the watched folder

The next step would be to activate the PDF Suite service. Please open the services control panel and configure the PDF Suite service to startup automatic. Furthermore you need to remove the Aloaha shortcut from the autostart/startup group of the Windows Menu.

Now you are ready to configure the hot folder. Please follow the steps below to configure the watched folder

1. Create a plain text file (i.e. crypto.ini). The file will contain the Filepath(s) to the hotfolder configuration file. Additional you need to create a registry entry of type string in HKLM\Software\Aloaha\pdf with name crypterini. The value is of type string and contains the path to this file.

For example c:\program files\wrocklage\crypto.ini

The file itself will look like the sample below:

c:\cryptohotfolder\management.ini

c:\cryptohotfolder\humanresources.ini

(one line/per hotfolder required)

2. The files defined above will contain the settings of the specified hotfolder. Please create a section called [encrypt] and create the following values:

infolder=c:\inputfiles

outfolder=c:\outputfiles

certpath1=c:\publickeys\humanresources.cer

certpath2=c:\publickeys\systemadministrator.cer

certpath3=c:\publickeys\management.cer

Every PDF file dropped in infolder will be encrypted with the certificates specified and moved to outfolder.

9. Aloaha Key Finder

Myriads of independent PKI services exist nowadays. Besides the well known commercial and freeware services even most governments are setting up their own PKI structures.

To be able to send somebody an encrypted email or PDF document the sender needs the public key/certificate of the recipient. In case you are on a regular basis in email contact with the recipient that is not a problem but consider the case you want to sell an eBook online. You might know only the email address of your customer but not the public key needed to encrypt the eBook.

The Aloaha Key Finder solves this problem. Several PKI LDAP Server can be configured in the ldap.txt and the key finder will query all configured servers for the public key correspondent to the given email address.

The executable version is included as a FREEWARE product in our Aloaha PDF Suite, Aloaha PDF Saver and Aloaha PDF Crypter. In case you need to use the Aloaha Key Finder ActiveX control please contact our sales department for a quotation.

10. FAQ

(look also <http://www.aloaha.de/support>)

What is the advantage of certificate based encryption?

Traditional password based PDF encryption is not safe at all. Owner passwords can be removed without even knowing the password. Tools like our Aloaha PDF Editor are able to remove passwords with just a click. An other advantage of certificate based encryption is that it can be defined who is allowed to open/view a document. It is not possible to forward a certificate secured document to a 3rd person.

How can I change the background image of the listboxes?

The images are located in the jpg subfolder. Just place your own images there.

How do I delete a profile?

As soon there is no active certificate left in a profile it will be deleted.

How do I import *.cer files?

Just drag and drop them into the certificate window

Does the Aloaha PDF Crypter support password protection of PDF documents?

No, the Aloaha PDF Crypter is a high security solution. Password protected PDF documents are not considered as secure. Our Aloaha PDF Editor for example is able to set/remove/change password protected PDF documents without having the password. The only secure protection against tampering of documents are digital signature. For digital rights management only certificate based encryption tools offer the needed security.

How do I embed other files to my PDF documents?

Before you encrypt the PDF document you can drag and drop any files into the files section. These files will be embedded automatically before encrypting the PDF document. You can also click on the label "Files to embed".

How do I use the Crypter OCX/ActiveX Component?

Sample source code is included in the samples\crypter subdirectory.

Why is my digital certificate not being listed?

There are two possibilities. Either your certificate properties do not allow to be used as an encryption certificate or your certificate is not located in the proper certificate store. In case your certificate is not allowed to be used for encryption you can apply for a free Class 1 Certificate at <http://pki.aloaha.com>

Why do I need certificate based PDF encryption?

Certificate based PDF encryption guarantees that only the intended recipient is able to open the PDF document. With password based encryption that could never be guaranteed since the password could be cracked, copied or forwarded to the 3rd party.

Why is the encrypt button greyed out when I drag a file into the files to attach box?

The files to attach are the files to be attached to the PDF Dokument. Not the PDF Dokument itself. The PDF Document to be encrypted should be specified with a click on the button with the 3 dots or just with dragging it left beside that button.

Can I encrypt PDF Files from within the Explorer with just a right click?

Yes, right click on the PDF File to encrypt and choose "Open With -> Choose Program". Then browse the the Aloaha PDF Crypter exe. From now on you can always with just a right click open your PDF in our PDFCrypter.

If you do not find your answer do not hesitate to contact us!

PDF based encryption is the ideal solution to publish eBooks, manage confidential documents or just to help you to get your database Sarbanes-Oxley compliant.

Index

- A -

Aloaha Public Key Finder 19
Application examples 17

- D -

Digital certificates 16

- F -

FAQ 20

- I -

Installation 5
Introduction 4

- P -

PDF Crypter Mailer 8
PDFCrypter Hotfolder 18
Personal search 15

- S -

Security 14

- U -

Usage 8