

WINDOWS

# Aloaha PDF Crypter



## **Aloaha PDF Crypter**

© 2010 Wrocklage Intermedia GmbH

# Aloaha PDF Crypter

© 2010 Wrocklage Intermedia GmbH

Copyright © 2009 Wrocklage Intermedia GmbH (im folgenden Wrocklage genannt). Alle Rechte vorbehalten. Der Inhalt dieses Dokumentes darf ohne vorherige schriftliche Genehmigung durch Wrocklage in keiner Form, weder ganz noch teilweise, vervielfältigt, weitergegeben, verbreitet oder gespeichert werden. Wrocklage entwickelt die Produkte im Rahmen eines kontinuierlichen Verbesserungsprozesses ständig weiter.

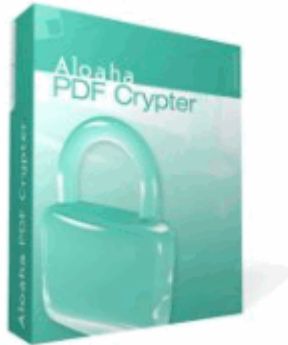
Wrocklage behält sich deshalb das Recht vor, ohne vorherige Ankündigung an jedem der in dieser beschriebenen Dokumentation beschriebenen Produkte Veränderungen bzw. Verbesserungen vorzunehmen. Wrocklage übernimmt keine Gewährleistung für technische oder redaktionelle Fehler oder Auslassungen in diesem Handbuch. Die Haftung für Schäden und Folgeschäden, welche auf einer leicht fahrlässigen Pflichtverletzung von Wrocklage eines gesetzlichen Vertreters und / oder Erfüllungsgehilfen von Wrocklage und auf der Verwendung dieses Dokumentes und der in ihm enthaltenen Informationen beruhen, ist ausgeschlossen, soweit keine Verletzung wesentlicher Vertragspflichten vorliegen. Wesentliche Vertragspflichten sind solche Pflichten, deren Erreichung die ordnungsgemäße Durchführung des Vertrages überhaupt erst ermöglichen und auf deren Einhaltung der Kunde regelmäßig vertrauen darf. Ansprüche aus dem Produkthaftungsgesetz bleiben hiervon unberührt. Der Inhalt dieses Dokumentes wird so dargelegt, wie er auch aktuell bekannt ist. Wrocklage übernimmt weder ausdrücklich noch stillschweigend irgendeine Gewährleistung für die Richtigkeit oder Vollständigkeit dieses Dokumentes.

Printed: Januar 2010

# Inhalt

	<b>Seite</b>
<b>1. Einleitung</b>	<b>4</b>
<b>2. Installation</b>	<b>5</b>
<b>3. Anwendung</b>	<b>7</b>
3.1. Funktionsweise des Aloaha PDF Crypter	12
<b>4. Sicherheit</b>	<b>13</b>
<b>5. Personensuche</b>	<b>14</b>
<b>6. Digitale Zertifikate</b>	<b>15</b>
<b>7. PDF Crypter Hotfolder</b>	<b>16</b>
<b>8. Aloaha Key Finder</b>	<b>17</b>
<b>9. Anwendungsbeispiele</b>	<b>18</b>
<b>10. FAQ</b>	<b>19</b>
<b>Index</b>	<b>21</b>

## 1. Einleitung



### Aloaha PDF Crypter Funktionen

PDF Verschlüsselung PDF 1.5 kompatibel (ab Adobe Reader 6).

Zertifikatsbasierte Verschlüsselung (X.509)

mehrere Zertifikate werden unterstützt.

Nur die Empfänger können das Dokument öffnen.

keine Kennwörter nötig.

Mehrere Empfänger sind möglich.

OCX Komponente ist enthalten.

ersetzt Passwortschutz

(Der Standard-Passwortschutz bei PDF Dateien ist sehr unsicher. z.B. können Besitzerpasswörter mit unserem Aloaha PDF Editor entfernt werden.

Dateien können als PDF Anhang eingebunden werden.

Integration in Windows Explorer.

Drag&Drop unterstützt.

incl. S/Mime Mailer

Verschlüsselte Dateien können direkt verschlüsselt und signiert per email mit dem eingebauten Mailer versandt werden.

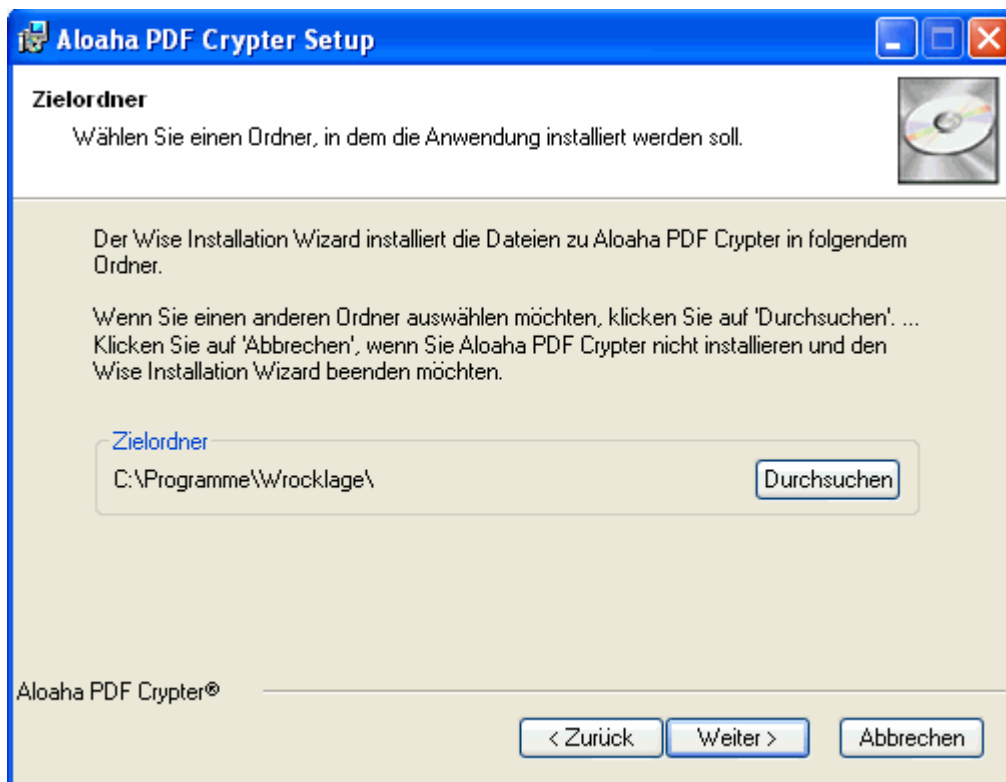
## 2. Installation

Um **Aloaha PDF Crypter** zu installieren, starten Sie die Installationsdatei (*aloaha\_crypter.exe*) per Doppelklick.

Nachdem die Sprache gewählt wurde, öffnet sich folgendes Dialogfenster.



Klicken Sie auf "Weiter" um das Installationsverzeichnis auszuwählen.

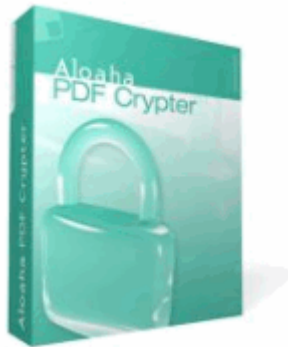


Um den vorgegebenen Zielordner zu verwenden, bestätigen Sie die Auswahl mit "*Weiter*" damit die Installationsroutine gestartet wird.  
Wählen Sie ggf. ein abweichendes Verzeichnis. Klicken Sie hierzu auf "Durchsuchen".

**Hinweis: Der Standard-Installationspfad kann meistens akzeptiert werden.**

Klicken Sie auf anschließend auf "*Fertigstellen*", damit die Installation abgeschlossen wird. In einigen Fällen müssen Sie den Computer neu starten, damit die Anwendungen wirksam werden und das System aktualisiert wird.

### 3. Anwendung



#### **Verschlüsseln Sie ihre PDF Dateien durch Zertifikate**

Mit dem Aloaha PDF Crypter verschlüsseln Sie Ihre PDF-Dateien mit Empfänger-Zertifikaten.

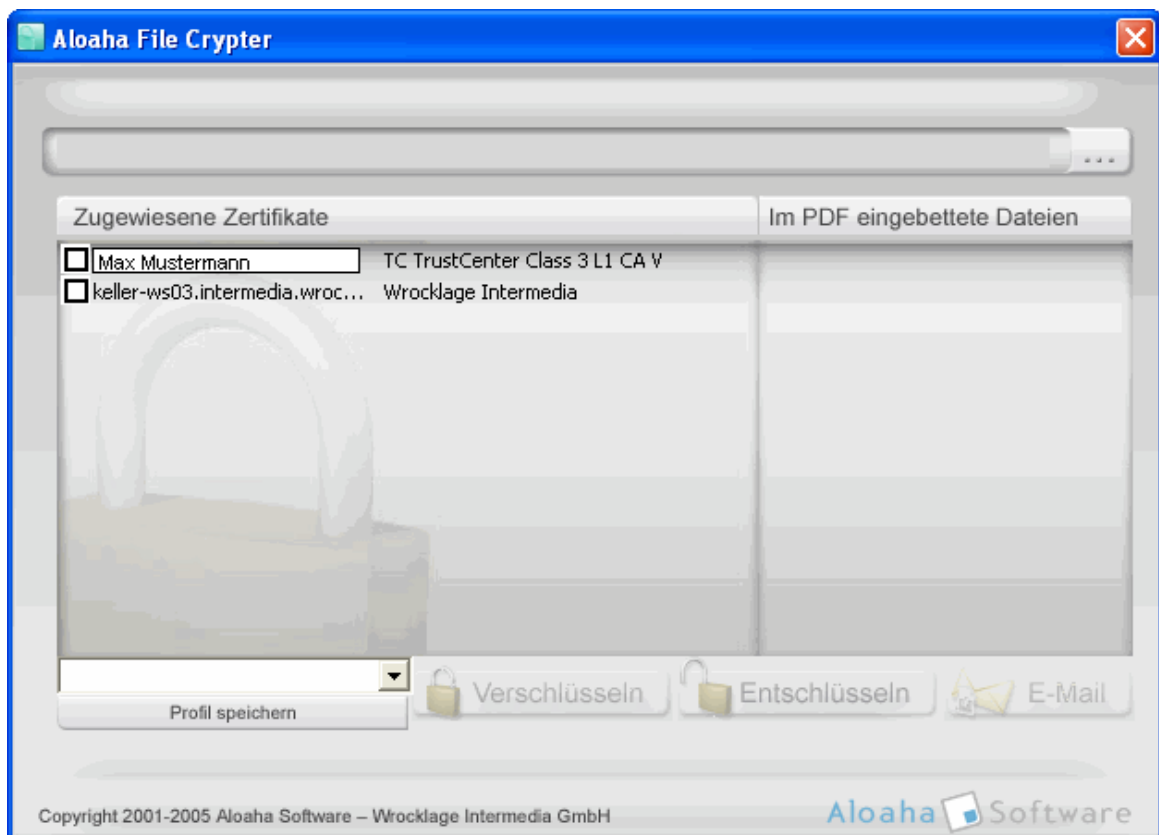
Öffnen Sie eine Datei, wählen Sie die Empfänger aus und klicken Sie auf "Verschlüsseln". Nun ist die Datei verschlüsselt und kann nur von den Empfängern geöffnet werden.

Endlich können Sie Ihre Verträge, Buchhaltungsunterlagen und andere vertrauliche Dokumente versenden, ohne dass jeder sie öffnen kann.

Der Aloaha PDF Crypter arbeitet nicht mit einem simplen Passwort sondern mit Zertifikaten. So ist ausgeschlossen, dass durch Ausprobieren von Kennwörtern die Datei "geknackt" werden kann.

Um Aloaha PDF Crypter zu starten, wählen Sie das Programm Aloaha PDF Crypter im Windows Startmenü.

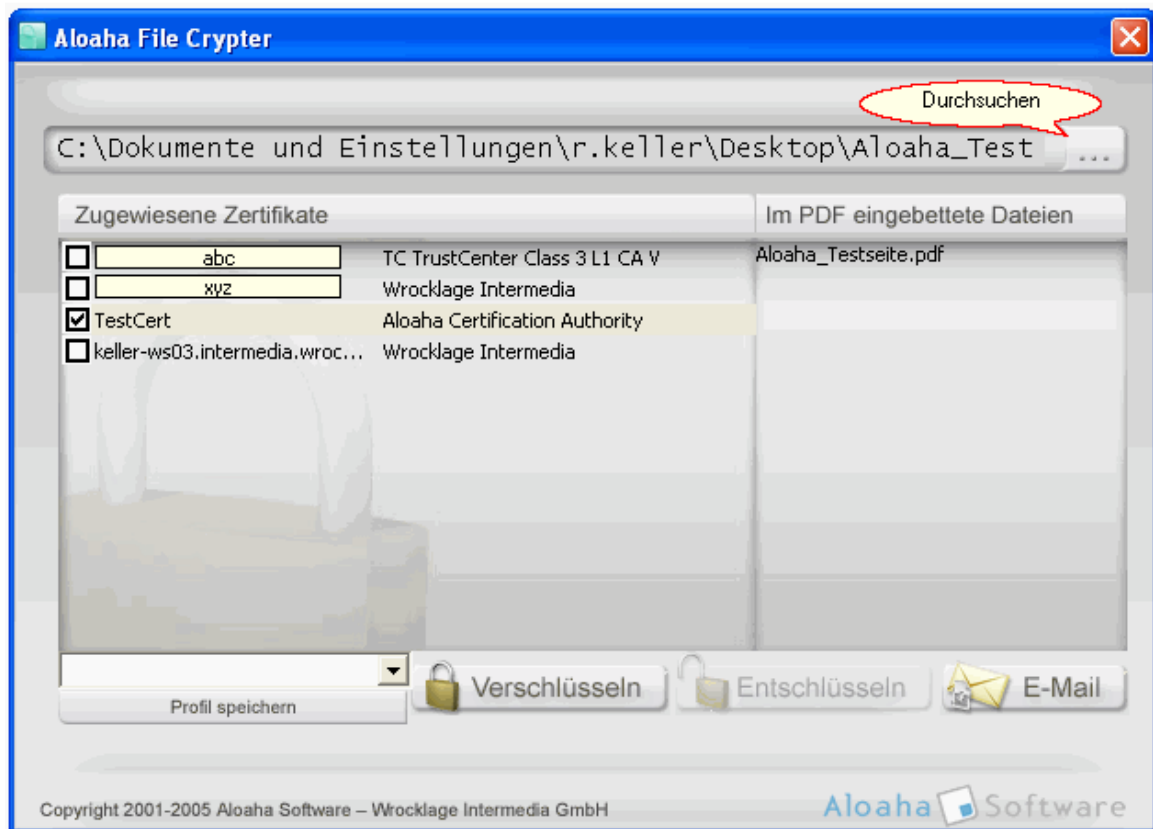
**Start>Alle Programme>Aloaha>Aloaha PDF Crypter**



Mit dem Aloaha PDF Crypter können Sie PDF Dateien ver- / entschlüsseln und ver- oder entschlüsselte Dateien per E-Mail versenden.

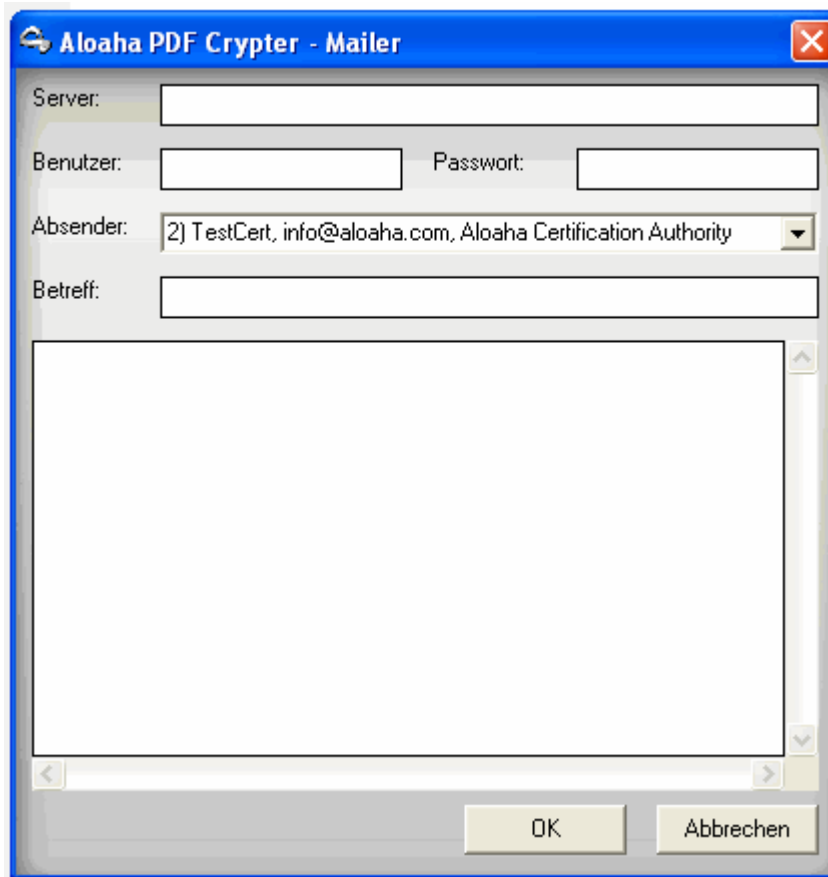
Wählen Sie das gewünschte Dokument welches verschlüsselt werden soll mit "Durchsuchen" in dem von Ihnen gewählten Ordner.

Anschließend wählen Sie das Zertifikat aus, welches zugewiesen werden soll. Mit einem Klick auf "Verschlüsseln" wird dem Dokument das entsprechende Zertifikat zugewiesen.



Nachdem Sie das Dokument ver- bzw. entschlüsselt haben, können Sie es bei Bedarf per E-Mail versenden.

Klicken Sie hierzu auf "E-Mail", anschließend öffnet sich der [PDF Crypter Mailer](#).



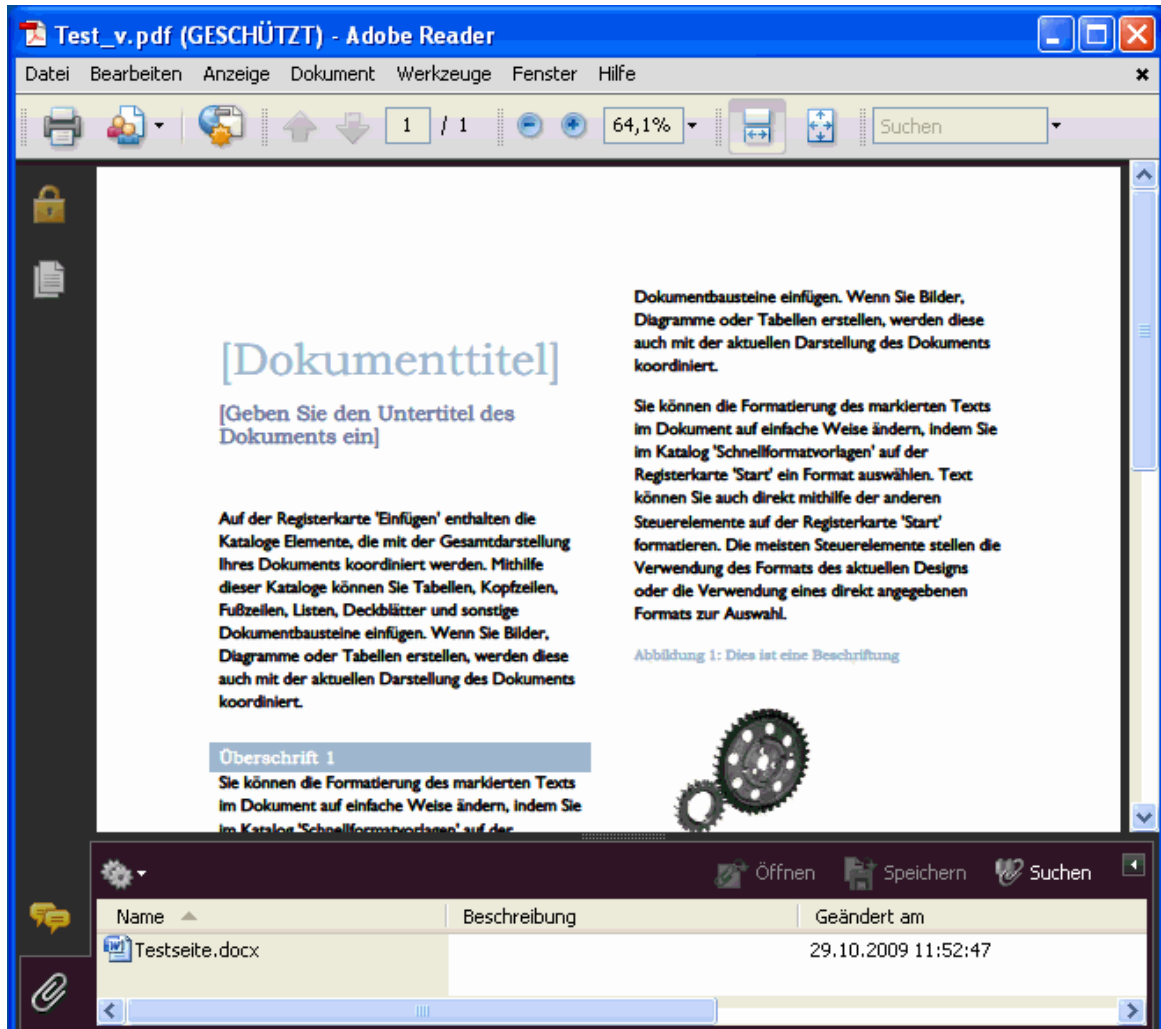
The image shows a Windows-style dialog box titled "Aloaha PDF Crypter - Mailer". It contains several input fields and a list box for configuring an email. The fields are:

- Server: [Empty text box]
- Benutzer: [Empty text box] Passwort: [Empty text box]
- Absender: [List box containing "2] TestCert, info@aloaha.com, Aloaha Certification Authority"]
- Betreff: [Empty text box]

Below these fields is a large empty text area for the email body. At the bottom of the dialog are two buttons: "OK" and "Abbrechen".

Sie können auch Dateien in das PDF eingebetten, welche mit dem PDF Dokument verschlüsselt werden.

Wenn Sie das PDF Dokument anschließend mit dem Adobe Reader öffnen, sehen Sie zusätzlich die im PDF eingebettete Datei.



### 3.1 Funktionsweise des Aloaha PDF Crypter

Hintergrund des Programms

#### Was passiert beim Verschlüsseln mit dem Aloaha PDF Crypter?

Das PDF Dokument wird mit den Public Keys der ausgewählten Empfänger verschlüsselt.

#### Wie funktioniert der Aloaha PDF Crypter?

Man wählt die Zertifikate links aus. Dann zieht man oben das PDF hinein und klickt auf verschlüsseln. Man kann auch Zertifikate hinzufügen indem man diese per Drag and Drop in die Zertifikatsliste verschiebt. Rechts daneben kann man noch per Drag and Drop Dateien „hinzufügen“. Diese werden vor dem Verschlüsseln als Anhang in das PDF Dokument eingefügt.

#### Wie funktioniert das kryptografische Verschlüsseln?

Man verschlüsselt mit dem Public Key und somit kann das PDF nur vom Besitzer des "private Keys" geöffnet werden.

## 4. Sicherheit

### Sicherheit durch digitale Zertifikate

Die Sicherheit wird durch das Verwenden des öffentlichen Schlüssels Ihrer elektronischen Unterschrift erreicht.

Der bzw. die Empfänger können dann die PDF Datei mittels Adobe Reader ab Version 6 lesen.

Im Gegensatz zu passwortgeschützten PDF Dateien kann die Zertifikatssicherheit nicht mit Zusatzprogrammen umgangen werden.

### Sicherheit in PDF Dateien

PDF Dateien werden mit Adobe Reader 6 und Adobe Reader 7 kompatibel verschlüsselt. Der Empfänger braucht also keine zusätzliche Software um das Dokument betrachten zu können.

### Sicherheit in nicht-PDF Dateien

Nicht-PDF-Dateien werden als Aloaha Dateien gespeichert. Vorher werden sie verschlüsselt und komprimiert. Um diese Dateien zu entschlüsseln ist der Aloaha PDF Crypter erforderlich. Die Ver- und Entschlüsselungsfunktionen für Nicht-PDF-Dateien sind freie Funktionen, wofür keine Lizenz erforderlich ist.

## 5. Personensuche

### Suche nach Personen

Manchmal ist es notwendig, ein verschlüsseltes Dokument an Personen zu versenden, deren Public Key und/oder E-Mail-Adresse nicht bekannt ist. Leider gibt es keine Datenbank, wie z.B. ein Telefonbuch, um nach diesen Informationen zu suchen.

Public Keys können via LDAP in der PKI (Public Key Infrastruktur), die der Empfänger benutzt, gefunden werden. Falls Sie die PKI des Empfängers nicht kennen, können sie den Aloaha Key Finder benutzen.

Der Aloaha Key Finder benutzt eine einfache Textdatei, die eine Liste der populärsten PKIs enthält und diese dann nach dem Public Key des Empfängers durchsucht.

### Windows-Suche nach Personen

Jede moderne Windows Version hat mittlerweile die Funktion "Suche nach Personen" integriert. Um nach Leuten zu suchen öffnen Sie einfach Ihr Windows Startmenü ->Suche->nach Personen ...

Wenn die gesuchte Person gefunden ist, kann auf den Public Key zugegriffen werden, welcher dann in die Tabelle der Digitalen IDs exportiert werden kann.

Aus der allgemeinen Tabelle können Sie die Person zu Ihrem Adressbuch hinzufügen, wodurch dem Aloaha PDF Crypter der Zugriff auf deren Public Key ermöglicht wird.

## 6. Digitale Zertifikate

### Digitale Zertifikate

Um auf Computern und im Internet eine Person korrekt zu identifizieren werden digitale Zertifikate oder auch eine digitale Unterschrift verwendet.

Zertifikate werden von Zertifizierungsstellen herausgegeben. Ein Zertifikat besteht immer aus zwei Teilen, dem privaten Schlüssel und dem dazugehörigen öffentlichen Schlüssel. Der öffentliche Schlüssel wird von der Zertifizierungsstelle (Trustcenter) verwaltet und in einem Verzeichnis veröffentlicht.

Wurde ein Dokument digital unterschrieben, kann der Empfänger die Echtheit des verschlüsselten Dokumentes anhand des öffentlichen und des privaten Schlüssels überprüfen.

Zertifikate werden in unterschiedlichen Sicherheitsstufen angeboten, welche in folgende Klassen eingeteilt sind:

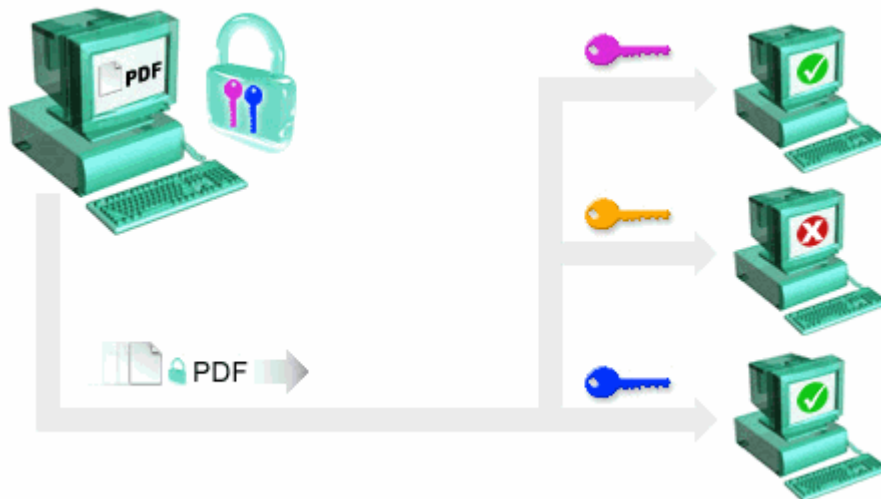
Klasse 0 Zertifikate sind normalerweise Testzertifikate ohne rechtlichen Hintergrund.

Klasse 1 Zertifikate bestätigen die Echtheit einer E-Mail-Adresse.

Klasse 2 Zertifikate bestätigen die Echtheit einer Organisation bzw. eines Unternehmens. Diese Zertifikate sind hauptsächlich für die gesicherte Kommunikation zwischen bereits bekannten Partnern gedacht.

Klasse 3 Zertifikate sind die sichersten Zertifikate und beinhalten eine persönliche Identitätsprüfung der Person. Die Person wird dabei anhand eines gültigen Ausweises identifiziert und die Zertifizierungsstelle stellt sicher, dass die im Zertifikat enthaltenen Angaben zur Person mit den Angaben im Ausweis übereinstimmen.

Nach der Überprüfung durch die Zertifizierungsstelle wird das Schlüsselpaar an den Benutzer ausgeliefert (z.B. auf einer Chipkarte per Post) und das Zertifikat veröffentlicht. Danach kann mit der entsprechenden Software jedes Dokument digital unterschrieben werden.



## 7. PDF Crypter Hotfolder

In Unternehmensumgebungen könnte es notwendig sein, den Verschlüsselungsprozess zu automatisieren. Online-Buchhandlungen können Aloaha PDF Crypter über die Crypter API in ihrem \*.NET, ASP oder PHP Webshop integrieren. Das Aloaha PDF Crypter API ist nur in der Unternehmensausgabe verfügbar.

Viel populärer als Aloaha Crypto-API ist der Aloaha Crypter Hotfolder.

**The Aloaha PDFCrypter watched folder allow defining a folder to encrypt any PDF document dropped into that folder with the public keys configured.** Die Dropfolder Funktionalität ist in der Server-Version verfügbar.

Die Aloaha Crypto Ordner sind der ideale Weg, ihre PDF-Dokumente zuverlässig zu verschlüsseln, bevor diese in den PickUpFolder Ihres Dokumentenverwaltungssystems verschoben werden.

### Konfiguration des Aloaha PDF Crypter Hotfolder

Um in der Lage zu sein, einen Hotfolder zu verwenden, ist ein Mechanismus erforderlich der diese Ordner überwacht. Um die Konfiguration einfach zu gestalten, nutzt Aloahas PDF Crypter den Hotfolder Mechanismus der Aloaha PDF-Suite. Installieren Sie dafür die Aloaha PDF-Suite von [http://www.aloaha.com/download/aloaha\\_pdf.zip](http://www.aloaha.com/download/aloaha_pdf.zip)

Als nächsten Schritt aktivieren Sie den PDF-Suite-Service. Klicken Sie zuerst mit der rechten Maustaste auf das Aloaha Systray Icon und beenden Sie Aloaha. Öffnen Sie das Service Control Panel und konfigurieren Sie den PDF-Suite-Service, um das Programm automatisch zu starten. Außerdem müssen Sie den Aloaha Shortcut aus der Gruppe Autostart im Windows Startmenü entfernen. Starten Sie den PDF-Suite-Service und vergewissern Sie sich mit einem Klick der rechten Maustas auf das Aloaha Icon, ob "Interaktiv" deaktiviert ist!

Nun sind Sie soweit den Hotfolder zu konfigurieren. Folgen Sie den Schritten, um den überwachten Ordner zu konfigurieren.

1. Erstellen Sie eine Klartext-Datei (d. h. crypto.ini). Diese Datei enthält den Pfad zur Hotfolder Konfigurationsdatei. Zusätzlich müssen Sie einen Registrierungszugang des **Typ-Schnur (type string)???** in HKLM\Software\Aloaha\pdf mit dem Namen `crypto.ini` anlegen. Der Wert ist von der **Typ-Schnur (type string)???** und enthält den Pfad zu dieser Datei.

Beispiel:

```
c:\program files\wrocklage\crypto.ini
```

Die Datei selbst wird wie das Beispiel unten aussehen:

```
c:\cryptohotfolder\management.ini
c:\cryptohotfolder\humanresources.ini
```

### Hinweis: Pro Hotfolder ist eine Zeile erforderlich!!!

2. Die oben definierten Dateien enthalten die Einstellungen der angegebenen Hotfolder. Legen Sie einen Bereich [verschlüsseln] an und anschließend die folgenden Werte:

```
infolder=c:\inputfiles
outfolder=c:\outputfiles
certpath1=c:\publickeys\humanresources.cer
certpath2=c:\publickeys\systemadministrator.cer
certpath3=c:\publickeys\management.cer
```

Jede in den Eingangsordner verschobene PDF-Datei wird mit den angegebenen Zertifikaten verschlüsselt und in den Ausgangsordner verschoben.

## 8. Aloaha Key Finder

Heutzutage bestehen Myriaden von unabhängigen PKI Dienstleistern. Außer den bekannten kommerziellen lizenzfreien Software Dienstleistern stellen sogar die meisten Regierungen ihre eigenen PKI Strukturen auf.

Um in der Lage zu sein, jemandem eine verschlüsselte E-Mail oder PDF-Dokumente zu senden, braucht der Absender den öffentlichen Schlüssel/Zertifikat des Empfängers. Im Falle dass Sie mit dem Empfänger regelmäßig im E-Mail-Kontakt stehen, der nicht ein Problem ist, Sie aber in Betracht ziehen, ein eBook online zu verkaufen, sollten Sie wissen, dass nur die E-Mail-Adresse Ihres Kunden, nicht aber des öffentlichen Schlüssels des eBooks verschlüsselt werden muss. Der Aloaha Key Finder behebt dieses Problem. Mehrere PKI LDAP Server können in ldap.txt konfiguriert werden und der Key Finder wird alle konfigurierten Server für den Public Key zur angegebenen E-Mail-Adresse abfragen.

Die ausführbare Version ist als LIZENZFREIE SOFTWARE Bestandteil in unserer Aloaha PDF-Suite, dem Aloaha PDF-Saver und dem Aloaha PDF Crypter. Im Falle dass Sie den Aloaha Key Finder ActiveX verwenden müssen, setzen Sie sich bitte mit unserer Vertriebsabteilung für einen Kostenvoranschlag in Verbindung.

## 9. Anwendungsbeispiele

Aloaha PDF Crypter ist ideal für alle, die vertrauliche Dokumente verwalten müssen. Nur die Empfänger können die Dateien öffnen. Das ist z.B. für:

Banken (Kontoauszüge, etc)  
Rechtsanwälte (Verträge, Vertragsentwürfe)  
Buchhaltung (Bilanzen)  
Aussendienst (geheime Firmeninformationen)

kurz, für alle Informationen die z.B. per E-Mail an Empfänger ausserhalb des Unternehmens lesbar sein sollen, äusserst interessant.

## 10. FAQ

(siehe auch <http://www.aloaha.de/support>)

### Welchen Vorteil bietet die zertifikatbasierte Verschlüsselung?

Traditionelle passwortbasierte PDF Verschlüsselung ist nicht sicher. Kennwörter können entfernt/zurückgesetzt werden, ohne sogar das Kennwort zu wissen. Werkzeuge wie unser Aloaha PDF Editor sind in der Lage, Kennwörter mit einem Klick zu entfernen/zurückzusetzen. Ein weiterer Vorteil der basierten Verschlüsselung des Zertifikats besteht darin, dass definiert werden kann, wem erlaubt wird, ein Dokument zu öffnen/anzusehen. Es ist nicht möglich, ein durch ein Zertifikat gesichertes Dokument an eine dritte Person weiterzuleiten.

### Wie kann ich das Hintergrundbild der Listbox ändern?

Die Bilder sind im jpg Unterordner abgelegt. Legen Sie Ihre eigenen Bilder dorthin.

### Wie lösche ich ein Profil?

Sobald kein aktives Zertifikat im Profil existiert, wird das Profil gelöscht.

### Wie kann ich \*.cer-Dateien importieren?

Verschieben Sie die Dateien per Drag & Drop in das Zertifikat-Fenster.

### Unterstützt der Aloaha PDF Crypter den Passwortschutz von PDF Dokumenten?

Nein, der Aloaha PDF Crypter ist eine hohe Sicherheitslösung. Passwortgeschützte PDF Dokumente werden nicht als sicher nicht betrachtet. Der Aloaha PDF Editor ist ohne das Kennwort zu haben in der Lage, passwortgeschützte PDF Dokumente zu entfernen/zu ändern. Der einzige sichere Schutz von Dokumenten ist die Digitalunterschrift. Für das Digitalrecht-Management geben nur Zertifikat Verschlüsselungswerkzeuge die erforderliche Sicherheit.

### Wie kann ich andere Dateien in meine PDF Dokumente einbetten?

Bevor Sie das PDF-Dokument verschlüsseln können Sie Dateien per Drag & Drop in die Dateiablage verschieben. Diese Dateien werden vor dem Verschlüsseln automatisch das PDF-Dokumentes eingebettet. Sie können allerdings auch auf den Button "einzubettende Dateien" klicken.

### Wie verwende ich die Aloaha Crypter OCX/ActiveX Komponenten?

Beispiele hierzu sind im Installationsverzeichnis >><C:\Programme\Wrocklage\samples\crypter><< zu finden.

### Warum wird mein digitales Zertifikat nicht angezeigt?

Es gibt zwei Möglichkeiten. Entweder die Zertifikat-Eigenschaften erlauben nicht, als ein Verschlüsselungszertifikat verwendet zu werden oder Ihr Zertifikat ist nicht im richtigen Zertifikatspeicherort abgelegt.

Im Falle dass Ihrem Zertifikat nicht erlaubt wird, für die Verschlüsselung verwendet zu werden, können Sie ein kostenloses Zertifikat der Klasse 1 über <http://pki.aloaha.com> erwerben.

### Warum benötige ich eine zertifikatbasierte PDF Verschlüsselung?

Zertifikatgestützte PDF-Verschlüsselung garantiert, dass nur der beabsichtigte Empfänger im Stande ist, das PDF-Dokument zu öffnen. Bei der passwortbasierten Verschlüsselung, kann nicht garantiert werden, dass das Passwort geknackt, kopiert oder an Dritte weitergeschickt wird.

**Warum ist der Button "Verschlüsselung" abgedimmt, wenn ich eine Datei in die Box "zu verschlüsselnde Datei" verschiebe?**

Die anzuhängenden Dateien, sind die Dateien, welche dem PDF Dokument beizufügen sind, nicht das PDF Dokument selbst. Das zu verschlüsselnde PDF Dokument sollte mit einem Klick auf den Button mit den 3 Punkten (Durchsuchen) oder durch Ziehen neben diesen Button.

**Kann ich PDF Dateien vom Windows Explorer aus per Klick auf die rechte Maustaste verschlüsseln?**

Ja, klicken Sie mit der rechten Maustaste auf die PDF-Datei, um diese zu verschlüsseln (**> Öffnen mit ... > Programme**). Dann suchen Sie das Programm Aloaha PDF Crypter exe. Zukünftig können Sie ihr PDF Dokument durch einen Klick mit der rechten Maustaste im PDF Crypter öffnen.

**Falls Sie hier keine Antwort auf ihre Frage gefunden haben, zögern Sie nicht uns zu kontaktieren!**

# Index

## - A -

Aloaha Key Finder 17  
Aloaha PDF Crypter Funktionen 4  
Aloaha PDF Crypter Mailer 7  
Anwendung 7  
Anwendungsbeispiele 18

## - D -

Digitale Zertifikate 15

## - E -

Einleitung 4

## - F -

FAQ 19

## - I -

Installation 5

## - P -

PDF Crypter Hotfolder 16  
PDF Crypter Mailer 7  
Personensuche 14

## - S -

Sicherheit 13