



## **Aloaha Multisignator**

© 2010 Wrocklage Intermedia GmbH

# Aloaha Mulitsignator

© 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: Juni 2010 in (whereever you are located)

# Inhalt

|                                           | <b>Seite</b> |
|-------------------------------------------|--------------|
| <b>1. Einleitung</b>                      | <b>4</b>     |
| <b>2. Anwendung</b>                       | <b>5</b>     |
| <b>3. Installation</b>                    | <b>8</b>     |
| 3.1 Systemvoraussetzungen                 | 8            |
| 3.2 Installation                          | 9            |
| <b>4. Konfiguration</b>                   | <b>12</b>    |
| 4.1 Einstellungen                         | 13           |
| 4.1.1 Digitale Unterschrift               | 14           |
| 4.1.2 Automailer                          | 20           |
| 4.1.3 Globale Einstellungen               | 21           |
| 4.1.4 Verzeichnis Picker                  | 23           |
| 4.1.5 POP3 Einstellungen                  | 24           |
| <b>5. Digital signieren</b>               | <b>25</b>    |
| <b>6. Language.ini</b>                    | <b>27</b>    |
| <b>7. Aloaha Signatur-Service</b>         | <b>28</b>    |
| <b>8. Aloaha Commandline Signer (ACS)</b> | <b>31</b>    |
| <b>9. CryptoAPI</b>                       | <b>31</b>    |
| <b>10. Technische Informationen</b>       | <b>32</b>    |
| <b>11. FAQ Multisignator</b>              | <b>33</b>    |
| <b>12. Tipps und Tricks</b>               | <b>36</b>    |
| <b>Index</b>                              | <b>37</b>    |

## 1. Einleitung



Erzeugen Sie serverseitige Massensignaturen für die elektronische Rechnungsstellung. Nutzen Sie das immense Einsparpotenzial durch rechtskonforme elektronische Rechnungslegung!

Sparen Sie zukünftig hohe Kosten durch Einsparungen in Arbeitszeit, Briefpapier, Umschläge, Druck- und Portokosten. Durch den elektronischen Rechnungsversand verkürzt sich die Zustellungszeit und damit das Zahlungsziel.

Überzeugende Argumente, um auf elektronische Rechnungsstellung umzustellen.

Hierzu benötigen Sie allerdings eine professionelle Software wie den Aloaha Multisignator, welche kompatibel zu Ihrem Buchhaltungssystem ist und die ausgehende E-Rechnungen vollautomatisch mit qualifizierten Signaturen versieht. Weiterer Vorteil: Auch die Archivierungskosten sinken bei elektronischer Rechnungsstellung.

Im Gegensatz zu anderen Massensignatur-Lösungen unterstützt der Aloaha Multisignator von Haus aus eine Vielzahl qualifizierter Signaturkarten sowie Software-Zertifikate. Zusätzliche Chipkartentreiber sind also beim Aloaha Multisignator überflüssig!

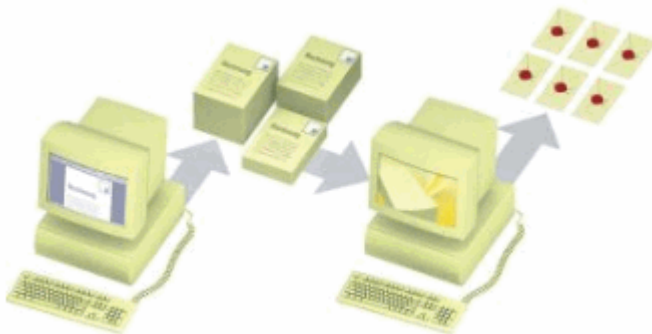
## 2. Anwendung

Der Aloaha Multisignator wurde entwickelt, um Massensignaturen durchzuführen und damit Ressourcen zu sparen.

### So funktioniert der Aloaha Multisignator

Die zu signierenden Ausgangsrechnungen werden einfach in einen Ordner des Computers kopiert. Dies kann automatisch durch Ihre Buchhaltungssoftware geschehen. Der Aloaha Multisignator versieht jede dieser Dateien mit einer elektronischen Signatur und versendet sie anschließend per E-Mail. Die E-Mailadressen können entweder aus dem PDF selbst ausgelesen werden oder mittels einer von der Buchhaltung erzeugten Kommandodatei übergeben werden. Auf Wunsch kann die E-Mail selbst noch signiert werden. Zur Erhöhung der Produktivität können mehrere Signaturkarten parallel angesteuert werden.

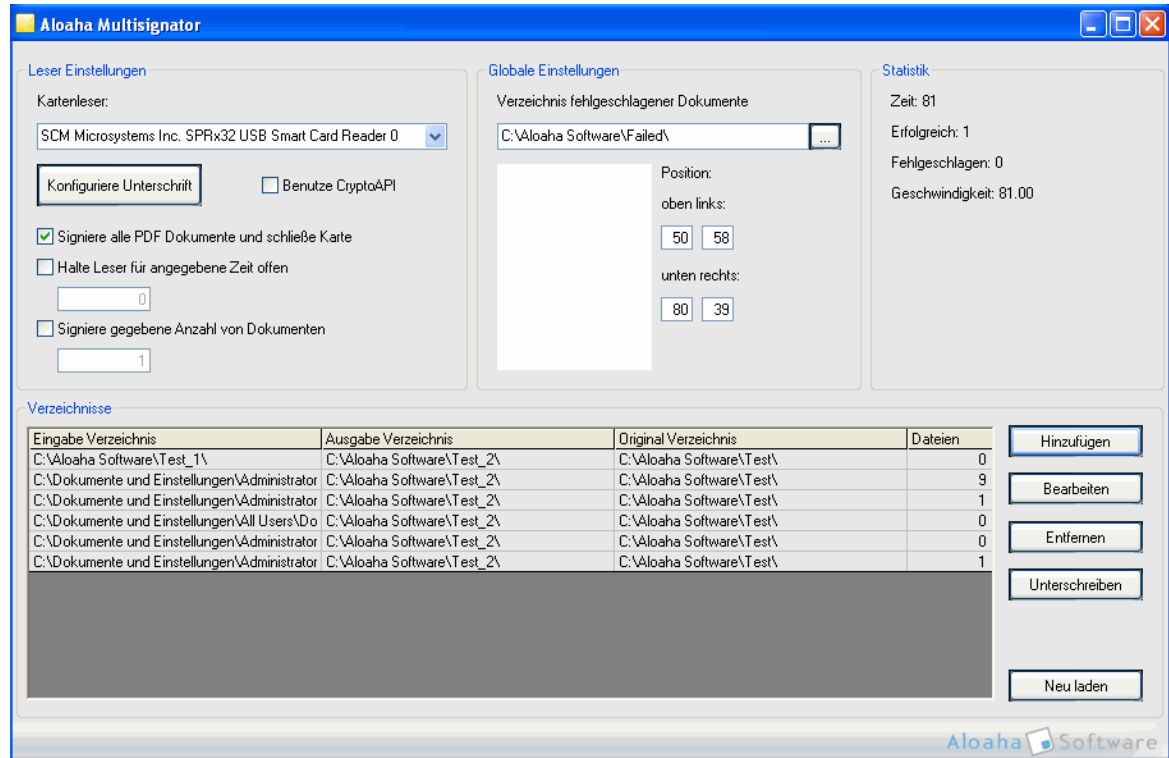
Bei Eingangsrechnungen nimmt der Aloaha Multisignator eine automatische Signaturprüfung vor. Bei negativer Prüfung informiert das System automatisch.



## Vorbereitung

Bevor Sie mit Massensignaturen beginnen, müssen nach Abschluss der Installation einige Einstellungen vorgenommen werden.

Nach dem Start des Programmes sehen Sie u.a. Bildschirm.



Zunächst müssen die entsprechenden **Verzeichnisse** mit den zu verarbeitenden Dokumenten angelegt werden.

Weiterhin sollten die **Leser Einstellungen** für den / die Kartenleser eingerichtet und die Signatur konfiguriert werden.

Je nachdem, ob Sie Dokumente über einen Zeitraum oder eine bestimmte Anzahl signieren möchten, ist das entsprechende Feld zu aktivieren.

Wenn Sie keine dieser Optionen anwenden möchten, aktivieren Sie "Signiere alle PDF Dokumente und schlieÙe Karte". Mit diesem Befehl werden alle Dokumente ohne Begrenzung signiert.

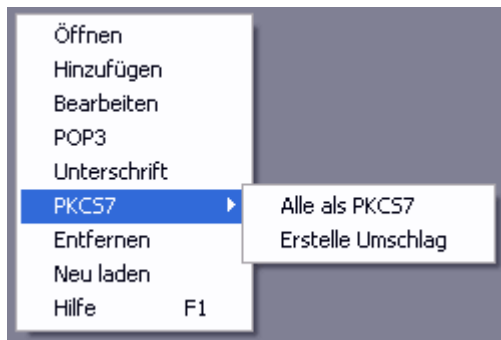
In den **globalen Einstellungen** legen Sie das Verzeichnis für fehlgeschlagene Dokumente fest. Hier werden Dokumente gespeichert, die nochmals bearbeitet werden müssen, da es bei der Massensignatur Probleme gegeben hat.

Weiterhin ist hier die **Position** und Größe des Signaturfeldes festzulegen.

Zu statistischen Zwecken werden folgende Parameter der erfolgten Massensignatur angezeigt:

Zeit:  
Erfolgreich:  
Fehlgeschlagen:  
Geschwindigkeit:

Wenn Sie mit der rechten Maustaste auf ein Eingangsverzeichnis klicken können Sie unter PKCS7 einstellen ob alle Dateien des Ordners PKCS7 signiert werden oder aber nur die nicht PDF Dateien. Weiterhin können Sie auswählen ob ein Umschlag erstellt werden soll oder eine externe Signaturdatei.



### 3. Installation



[Systemvoraussetzungen](#)  
[Installation](#)

#### 3.1 Systemvoraussetzungen

- Windows 2000, Windows 2003, Windows 2008, Windows XP, Windows Vista, Windows 7
- **Kein Adobe Reader erforderlich!**

## 3.2 Installation

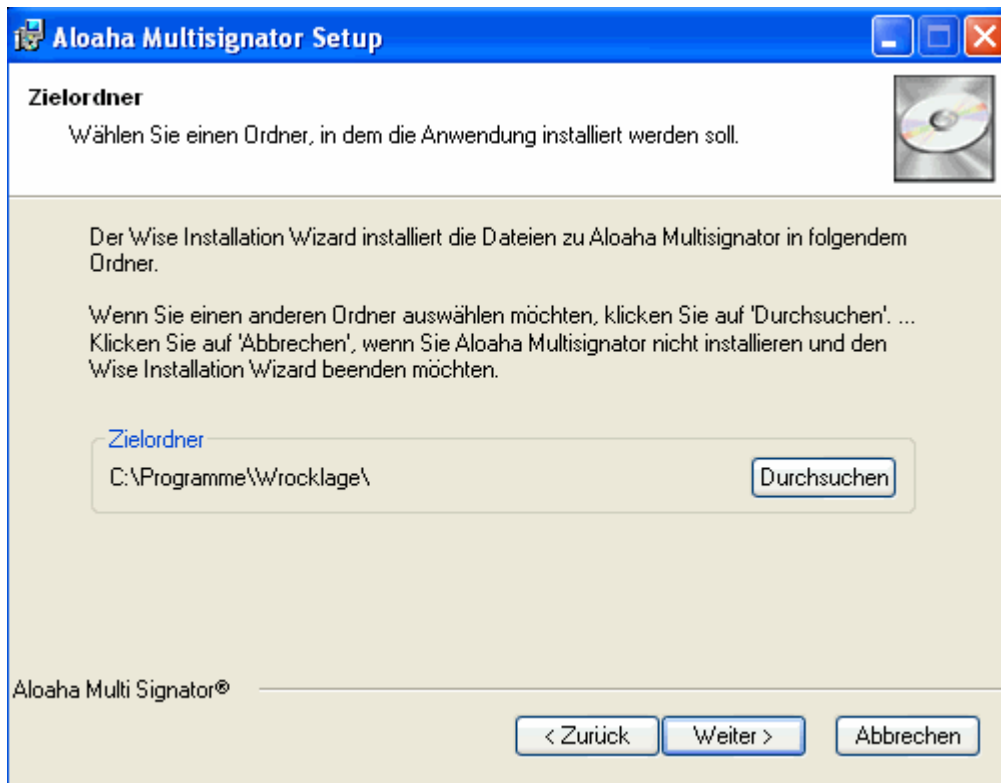
Den Aloaha PDF Multisignator können Sie sich direkt aus dem Internet unter [http://www.aloaha.com/download/aloaha\\_multisignator.zip](http://www.aloaha.com/download/aloaha_multisignator.zip) herunterladen.

Die Datei speichern Sie direkt auf Ihrer Festplatte. Sobald der Download beendet ist, entpacken Sie diese und doppelklicken auf "multisignator.exe".

Anschließend beginnen Sie die Software zu installieren.



Klicken Sie auf Weiter. Im nächsten Dialog wählen Sie bitte das Installationsverzeichnis. Standardmässig ist das auf c:\programme\wrocklage voreingestellt.



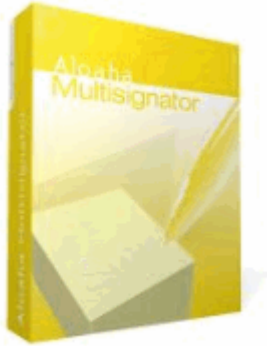
An dieser Stelle der Installation können Sie wählen ob Sie noch einmal einen Schritt zurück gehen möchten oder ob die Installation beginnen soll. Klicken Sie dazu auf zurück oder weiter.



Nach der erfolgreichen Installation schließen Sie den Installationsvorgang mit "Fertigstellen" ab.

Jetzt können Sie den Aloaha Multisignator verwenden. In Ihrem Startmenü unter Programme/ Aloaha finden Sie eine Verknüpfung zum Öffnen des Programmes.

## 4. Konfiguration



[Einstellungen](#)

[Tipps und Tricks](#)

[CryptoAPI](#)

[Digital Signieren](#)

[Language.ini](#)

[FAQ](#)

[Aloaha Signatur Service](#)

[Technische Informationen](#)

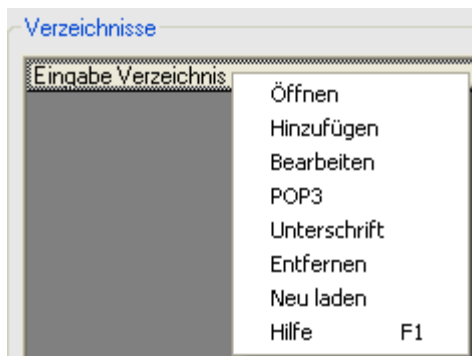
[Aloaha Commandline Signer](#)

## 4.1 Einstellungen



[Digitale Unterschrift](#)  
[Autemailer](#)  
[Globale Einstellungen](#)  
[Verzeichnis Picker](#)  
[POP3 Einstellungen](#)

Sämtliche Einstellungen können auch durch Klick mit der rechten Maustaste auf das Feld Verzeichnisse aufgerufen werden.



### 4.1.1 Digitale Unterschrift

Wenn Sie mit dem Aloaha Multisignator Dokumente digital signieren wollen, müssen Sie vorher einige Einstellungen vornehmen.

#### 1. Zertifikatsquelle

Hier können Sie zwischen den verschiedenen Arten von Zertifikaten wählen, die Sie gern zum Signieren Ihrer PDF-Dateien verwenden möchten. Zur Auswahl stehen:

##### Computer Zertifikate

- Es werden in der Zertifikats-Auswahlliste alle Zertifikate angezeigt, die dem Computer zugeordnet sind.

##### Benutzer Zertifikate (Standard)

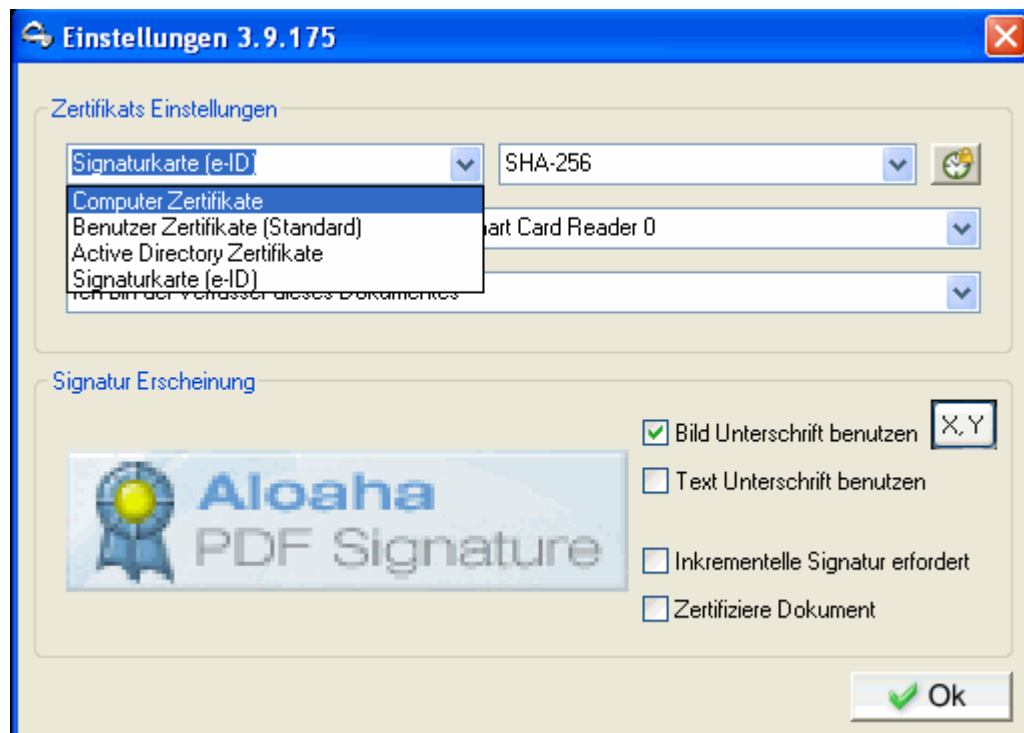
- Es werden in der Zertifikats-Auswahlliste alle Zertifikate angezeigt, die dem aktuellen Benutzer zugeordnet sind. Dieses ist die empfohlene Einstellung!

##### Active Directory Zertifikate

- Es werden in der Zertifikats-Auswahlliste alle Zertifikate angezeigt, die im Active Directory zur Verfügung stehen.

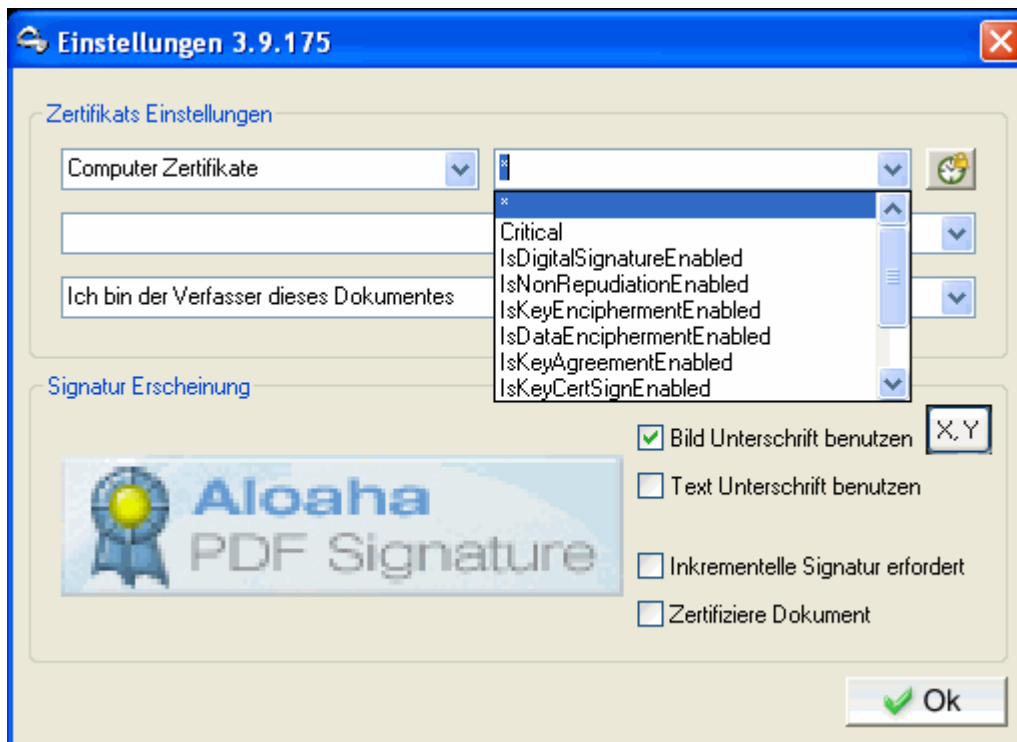
##### Signaturkarte (e-ID)

- Es werden in der Zertifikats-Auswahlliste alle angeschlossenen Kartenleser angezeigt. Bei nativ unterstützten Karten ist dieses die empfohlene Einstellung.



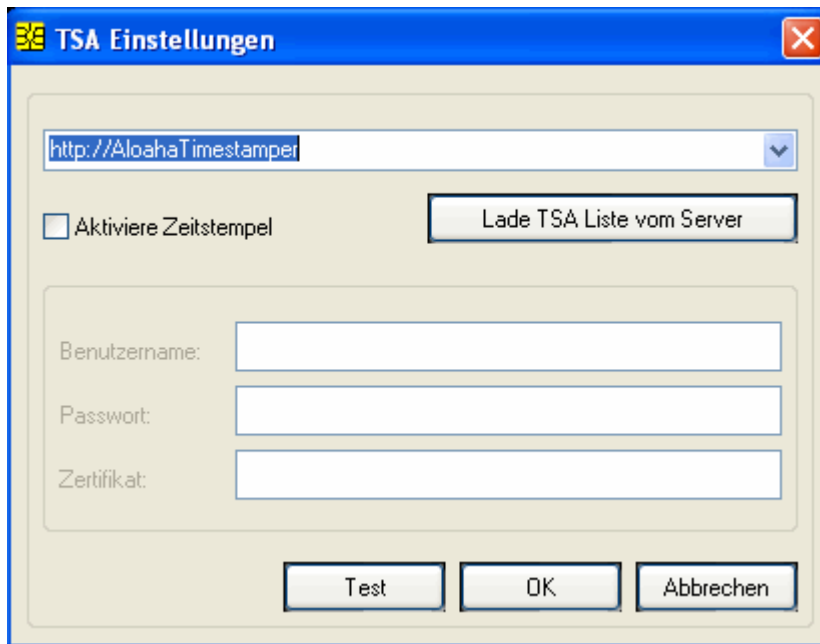
## 2. Art des Zertifikats

Hiermit können Sie die Zertifikatsliste der angezeigten Zertifikate nach besonderen Zertifikat-Attributen filtern. Wenn Signatur (e-ID) ausgewählt ist kann hier zwischen SHA-1 und SHA-256 gewählt werden!



### 3. Einstellungen für den Zeitstempel

Wenn Sie auf das Uhren-Symbol neben dem Filterfeld klicken öffnet sich ein weiteres Fenster:



Hier können Sie die Einstellungen für den integrierten RFC 3161 kompatiblen Zeitstempel Client anpassen.

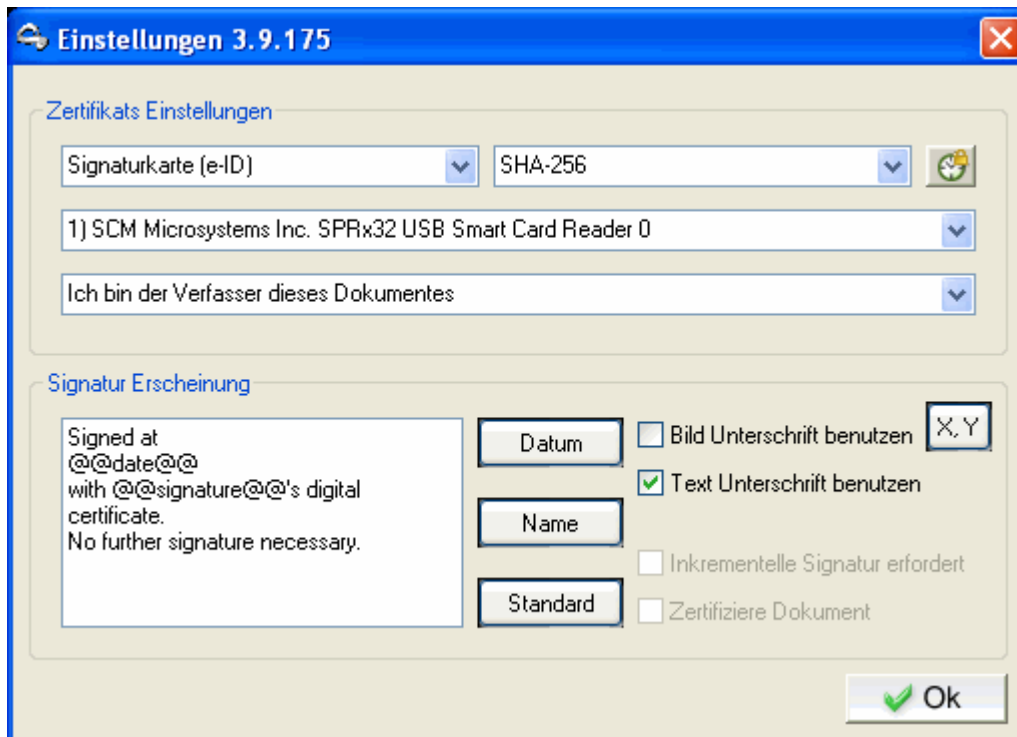
Im oberen Feld wählen Sie den Zeitstempelservers aus. Ist die Liste leer, können Sie die Liste der möglichen Zeitstempelservers durch Druck auf den Button "Lade TSA Liste vom Server" von der Aloaha Webseite herunterladen.

Wenn Sie `http://AloahaTimestamper` auswählen, so wird der in die Aloaha PDF Suite integrierte TimeStamp-Server benutzt. Hierbei wird die Lokale Systemzeit als Grundlage für den Zeitstempel genommen.

Unter Benutzerdaten konfigurieren Sie Ihre Zugangsdaten zum jeweiligen Zeitstempeldienst.

## 4. Zertifikat auswählen

Dieses Menü hängt von der Zertifikatsquelle ab. Wählen Sie dort beispielsweise "Benutzerzertifikat", erhalten Sie in diesem Feld eine Auflistung aller Benutzerzertifikate auf Ihrem PC und können dort das entsprechende auswählen. Wählen Sie als Zertifikat die SmartCard (e-ID) Option, erscheint in diesem Menü eine Auflistung aller zur Zeit installierten SmartCard-Lesegeräten auf Ihrem Rechner. Der Aloaha PDF Multisignator erkennt selbstständig die in dem Kartenleser eingelegte Smart-Card und kann die Zertifikate von unterstützten Karten lesen.

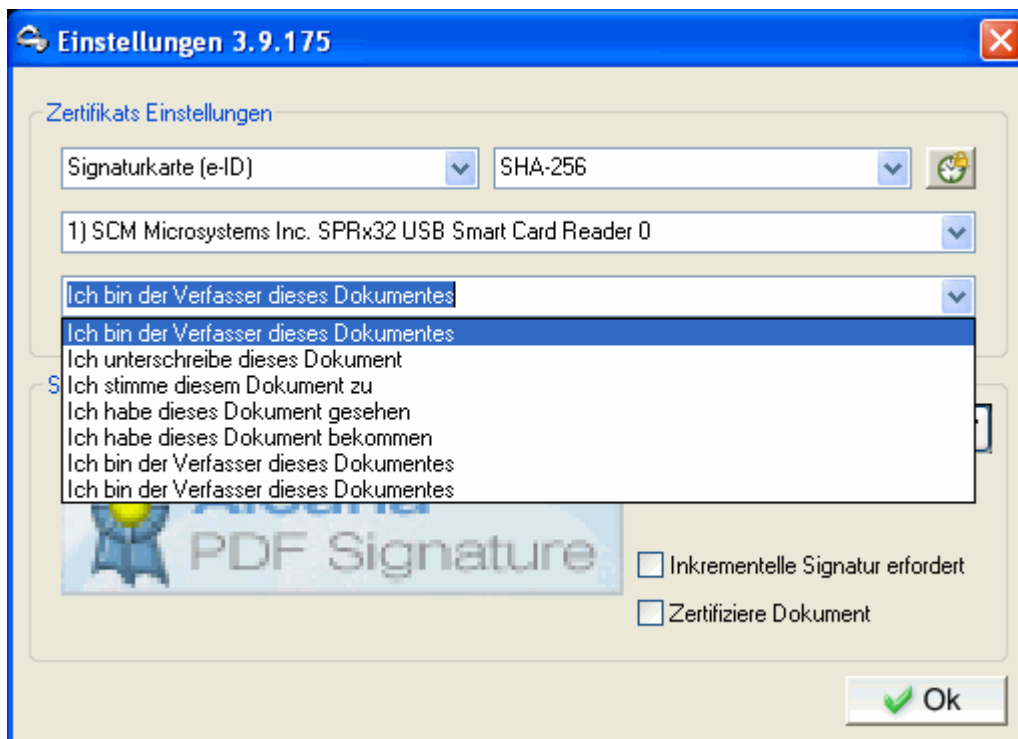


## 5. Zweck der Signatur

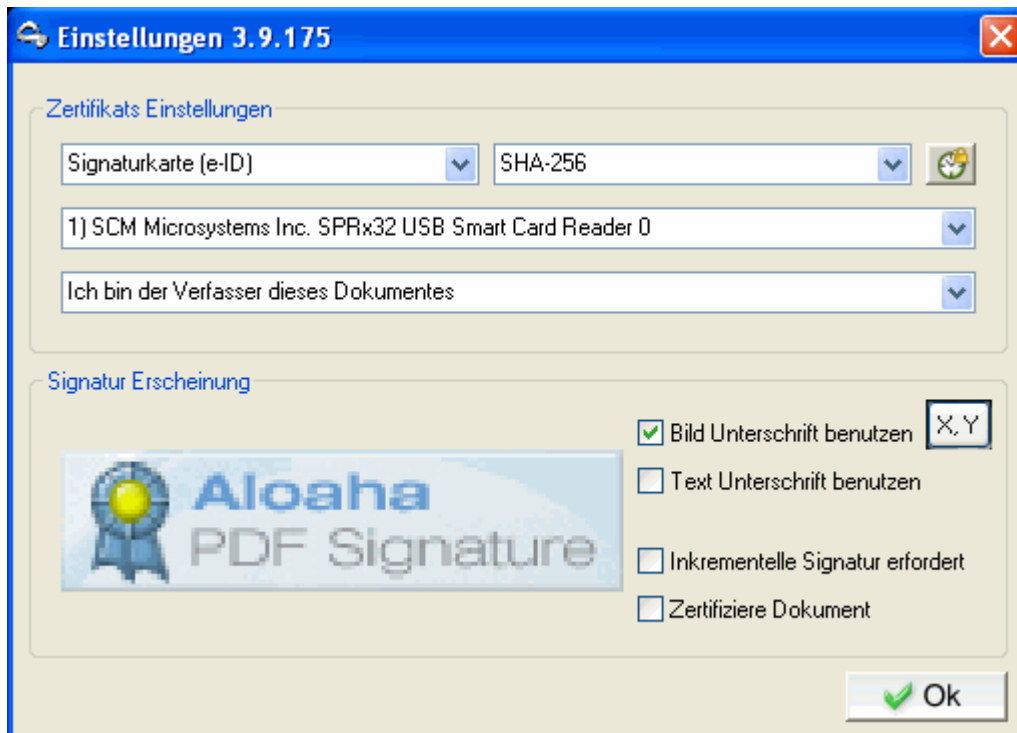
Hier können Sie aus mehreren Signaturen wählen, welche automatisch verwendet werden soll. Folgende Möglichkeiten stehen zur Auswahl:

- Ich bin der Verfasser dieses Dokumentes
- Ich unterschreibe dieses Dokument
- Ich stimme diesem Dokument zu
- Ich habe dieses Dokument gesehen
- Ich habe dieses Dokument bekommen

**Hinweis: Sie können natürlich auch eigenen Text eingeben!**



## 6. Erscheinung der Signatur



### **Bild Unterschrift benutzen**

Ist dieses Feld aktiviert, wird ein Bild in das PDF eingesetzt, so wie es die Vorschau in diesem Dialog zeigt. Durch Klick auf die Anzeige des aktuellen Unterschriftsbildes können Sie eine eigene Bild-Datei von Ihrer Festplatte laden. Dieses Bild muß im 24 Bit JPG Format sein und wird dann als Bild in das PDF gesetzt.

### **Text Unterschrift benutzen**

Ist diese Option aktiviert, wird der in dem darüber erscheinenden Feld eingegebene Text in das PDF eingesetzt. Sie haben die Möglichkeit, an der aktuellen Cursorposition durch Klick auf "Datum" und "Name" einen Platzhalter für Datum und Namen einzufügen. Hier wird dann im Signaturvorgang dieser Platzhalter durch das aktuelle Datum und der Name des Zertifikatinhabers ersetzt.

### **Inkrementelle Signatur erfordert**

Aloaha wird das Dokument inkrementell signieren. Dabei wird die Signatur so an das Dokument angehängt das sich jederzeit das Originaldokument wiederherstellen lässt!

## 4.1.2 Automailer

**Aloaha Automailer Konfiguration**

**Mail Server**

Postausgangsserver: localhost Port: 25

Benutzername: Administrator Alias: Administrator

Passwort:

WebDAV

**Standard**

eMail: me@localhost

Name:

Betreff: Your PDF

**Verzeichnisse**

Eingabe Verzeichnis:

Ausgabe Verzeichnis:

### Mailserver:

Hier sind folgende Daten für Ihren Account einzutragen:

#### Postausgangsserver

#### Port

#### Ihr **Benutzername**

Ihr **Aliasname**, falls er nicht mit dem Benutzernamen gleich ist

Ihr **Passwort** zu dem Benutzernamen

ggf. **WebDAV** aktivieren, falls Sie für Ihre Dokumente einen WebDAV Server (wie z.B. Microsoft Exchange oder SharePoint Server) verwenden möchten.

### Standard:

**eMail** - E-Mailadresse des Empfängers

**Name** - Name des E-Mail Empfängers

**Betreff** - Thema zu den zu verschickenden signierten Dokumenten

### Verzeichnisse:

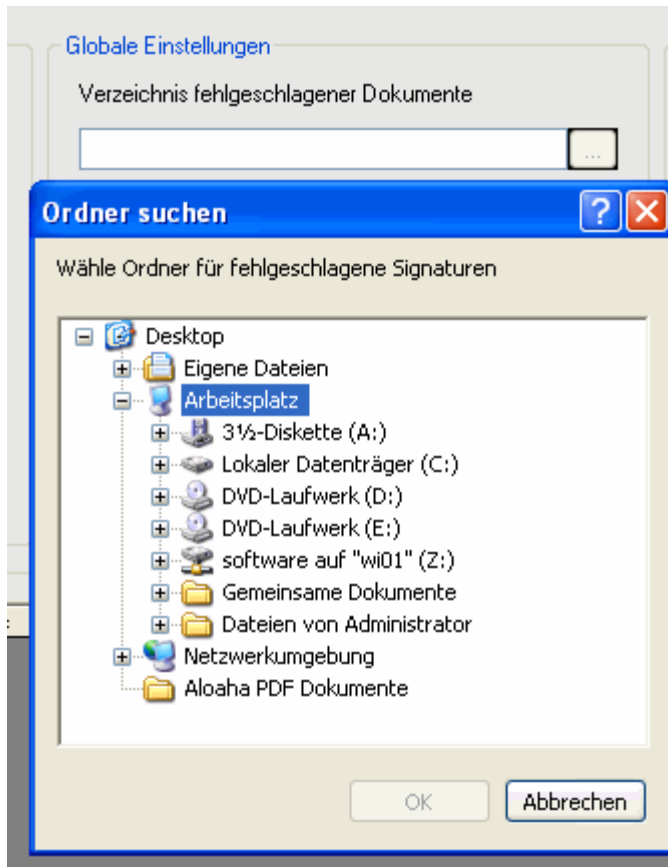
**Eingabe Verzeichnis** - Ist das Verzeichnis, aus welchem Aloaha die Dokumente lädt, um sie zu signieren.

**Ausgabe Verzeichnis** - Ist das Verzeichnis, in dem erfolgreich signierte Dateien abgelegt werden.

### 4.1.3 Globale Einstellungen

#### Verzeichnis fehlgeschlagener Dokumente:

Ist das Verzeichnis, in dem Aloaha die Dateien mit fehlgeschlagenen Signaturversuchen ablegt.

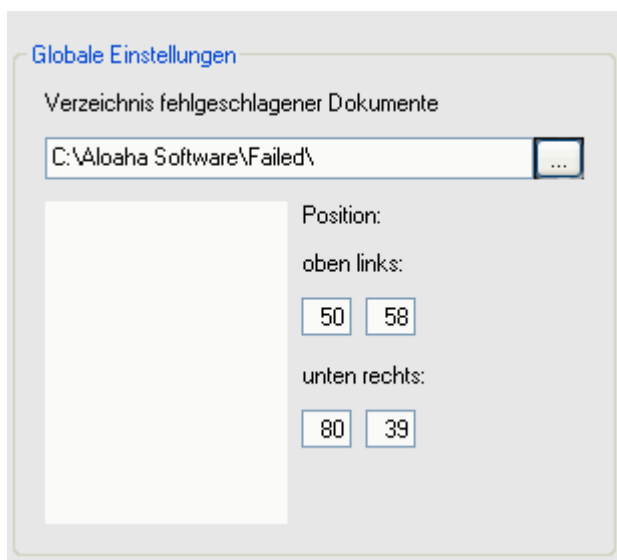


### Position der Signatur:

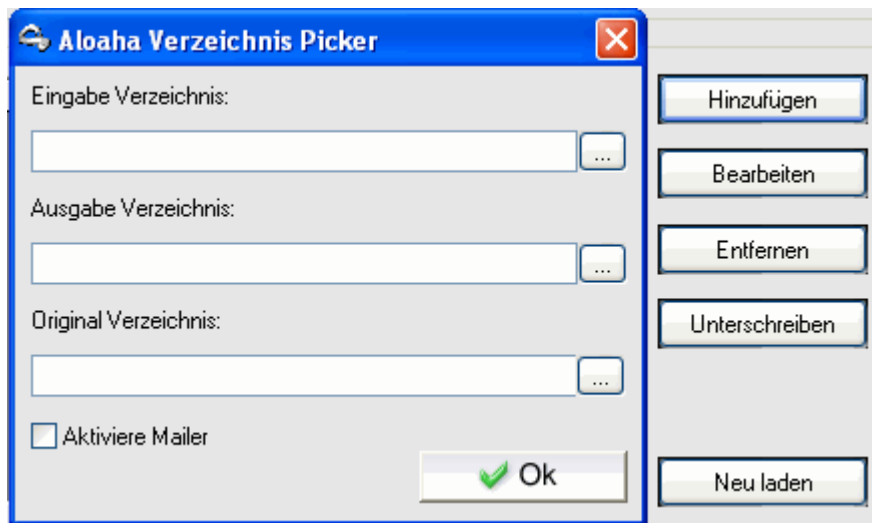
Hier werden Position und Größe des Signaturfeldes festgelegt.  
Die Position kann auch in den Signatureinstellungen festgelegt werden.

In den vier Feldern geben Sie die Position der Signatur vor. Hierbei wird immer in % der Seitengröße gerechnet. Das Koordinatensystem startet mit 0% links unten auf dem PDF. Unter "oben links" konfigurieren Sie die linke obere Ecke des Signaturfeldes, angefangen in der X-Achse. Unter "unten rechts" stellen Sie die Position der unteren rechten Ecke des Signaturfeldes ein. Wenn also in allen Feldern 45 eingetragen wird, erscheint das Feld in der Mitte des Blattes.

Alternativ können Sie die Position auch mit der Maus bestimmen. Klicken Sie mit der rechten Maustaste um die bisherige Wahl zu löschen. Fahren Sie mit der Maus die gewünschte obere linke Ecke der gewünschten Position an und klicken mit der linken Maustaste. Danach fahren Sie die rechte untere gewünschte Position an und klicken mit der linken Maustaste. So haben Sie die Position dann festgelegt.



#### 4.1.4 Verzeichnis Picker



##### **Eingabe Verzeichnis:**

Ist das Verzeichnis, aus welchem Aloaha die Dokumente lädt, um sie zu signieren.

##### **Ausgabe Verzeichnis:**

Ist das Verzeichnis, in dem erfolgreich signierte Dateien abgelegt werden.

##### **Original Verzeichnis:**

Hier werden nach erfolgter Signatur Originaldokumente abgelegt.

##### **Hinzufügen:**

Öffnet den Verzeichnis Picker, um weitere Ordner mit zu signierenden Dokumenten hinzuzufügen.

##### **Bearbeiten:**

Öffnet den Verzeichnis Picker, um ggf. den Eingabe-, Ausgabe- oder Originalordner zu ändern.

##### **Entfernen:**

Entfernt die von Ihnen angelegten Verzeichnisse aus der Ansicht

##### **Unterschreiben:**

Fordert Sie zur Eingabe Ihrer PIN auf, um das / die anstehenden Dokumente zu signieren.

##### **Neu laden:**

Lädt die zu signierenden Dateien aus den entsprechenden Ordnern neu

##### **Aktiviere Mailer:**

Ist die Option "Aktiviere Mailer" aktiviert, öffnet sich die Automailer Konfiguration. Hier können Sie die entsprechenden Optionen ggf. anpassen oder übernehmen (siehe hierzu auch [Automailer](#)).

### 4.1.5 POP3 Einstellungen

**Global**

POP3 Frequenz (sekunden): 60 Max. POP3 Prozesse: 3

**C:\Aloaha Software\Test\_1\'**

Server: localhost Port: 110

Benutzer: POP3 Frequenz: 300

Passwort: Max. downloads: 10

Mail Empfänger:  Sender in Kopie

Drop Verzeichnis: C:\Aloaha Software\Test\_1\'

Ok

#### Pop3 Frequenz (Sekunden):

POP3Frequency (Sekunden) definiert, in welchem Zeitfenster das POP3 Modul aufgerufen wird.

#### Max. Pop3 Prozesse:

Max. POP3 Prozesse definiert, wie viele POP3-Prozesse gestartet werden.

#### Server:

Definiert, welcher Server verwendet wird.

#### Benutzer:

Definiert den Anwender

#### Passwort:

Definiert das dem Anwender zugewiesene Passwort

#### Mail Empfänger:

Gibt an, an wer ggf. Mails erhalten soll

#### Drop Verzeichnis:

Gibt das Eingabeverzeichnis an

#### Port:

Gibt an, welcher Port verwendet werden soll.

#### Pop3 Frequenz:

POP3 Frequenz definiert, wie häufig einem POP3 Server erlaubt wird, in den Modus "Verbinden" gesetzt zu werden.

#### Max. Downloads:

Max Downloads definiert, wie viele E-Mails aus dem Posteingang heruntergeladen werden.

#### Sender in Kopie:

Wenn "Sender in Kopie" aktiviert ist, wird jede E-Mail dem Absender ebenfalls zugestellt.

## 5. Digital signieren

### PDF-Dateien elektronisch unterschreiben

Mit dem Aloaha PDF Saver können Sie PDF-Dateien digital signieren. Es wird eine elektronische Unterschrift nach den Vorgaben des Signaturgesetzes (SigG) der Bundesrepublik Deutschland unterstützt.

So können auch rechtskräftige elektronische Rechnungen mit dem Aloaha PDF Saver erstellt werden.

Rechnungen, die per Fax oder E-Mail übermittelt und/oder zum Download im Internet bereitgestellt werden (z. B. als PDF-Dokument) und keine "qualifizierte elektronische Signatur" tragen, stellen keine Rechnung im Sinne des Paragraphen 14 Abs. 3 Umsatzsteuergesetz dar.

Die von dem Aloaha PDF Saver erstellten digitalen Signaturen werden im PDF-Dokument eingebettet und können mit der freien Acrobat Reader ab Version 6 überprüft werden.

### Die digitale Signatur

Eine digitale Signatur im Sinne des Gesetzes ist „ein mit einem privaten Signaturschlüssel erzeugtes Siegel zu digitalen Daten, das mit Hilfe eines zugehörigen öffentlichen Schlüssels, der mit einem Signaturschlüssel Zertifikat einer Zertifizierungsstelle versehen ist, den Inhaber des Signaturschlüssels und die Unverfälschtheit der Daten erkennen lässt“ (SigG).

Mit der Entwicklung der digitalen Signatur wurde das Ziel verfolgt, eine der persönlichen Unterschrift äquivalente Signierungsmethode zu entwickeln, mit der auf elektronischem Wege Daten unterzeichnet werden können.

Das Hauptproblem bei der Übermittlung elektronischer Daten ist die leichte Manipulierbarkeit. Erst durch die elektronische Signatur konnte dieses Problem behoben werden, da eine unbemerkte Manipulation der Daten nicht mehr möglich ist.

Voraussetzung hierfür ist, dass die elektronische Signatur wie eine handschriftliche Unterschrift untrennbar mit dem jeweiligen Dokument verbunden ist. Sie kann von jedem eingesehen, aber nur vom Unterzeichner selbst geändert werden. Der Unterzeichner kann somit eindeutig identifiziert werden und die Signatur macht jede eventuelle Manipulation, wie das nachträgliche Streichen oder Ändern von Textpassagen eines Dokuments, sofort erkennbar.

Durch die Zertifikatsprüfung kann zudem bewiesen werden, dass die Signatur nicht gefälscht wurde und der Zertifikatsinhaber somit echt ist. Dabei werden außer seinem Namen keine persönlichen Daten preisgegeben..

### Gesetzliche Regelungen

Definitionen der unterschiedlichen Arten der digitalen Signatur finden sich im Signaturgesetz (SigG) und in der Verordnung zum Signaturgesetz (SigV). Außerdem werden darin Anforderungen an die elektronischen Unterschriften dargestellt sowie Zertifizierungsdiensteanbieter (ZDA) definiert.

Es wird unterschieden in **einfache**, **fortgeschrittene** und **qualifizierte digitale Signaturen**. Jede Signatur steht für eine bestimmte Qualitätsstufe. Je höherwertiger die Signatur, desto mehr Bedeutung hat sie für den Rechtsverkehr, und desto größer ist ihre Funktionalität.

Nur qualifizierte Signaturen erfüllen die Anforderungen in Bezug auf elektronische Daten genauso wie die handschriftliche Unterschrift Anforderungen in Bezug auf Daten in Papierform erfüllt. Sie sind sogar vor Gericht als Beweismittel zugelassen.

Die für qualifizierte elektronische Signaturen zugelassenen kryptografischen Algorithmen werden von der Bundesnetzagentur genehmigt und veröffentlicht. Unter [www.bundesnetzagentur.de](http://www.bundesnetzagentur.de) finden Sie zudem eine Liste aller akkreditierten Zertifizierungsdiensteanbieter (Trustcenter). Dort sind auch die für eine qualifizierte elektronische Signatur zugelassenen Produkte aufgelistet.

Die Voraussetzungen für eine qualifizierte Signatur sind dann gegeben, wenn sie ausschließlich dem Unterzeichner zugeordnet werden kann, die eindeutige Identifizierung des Unterzeichners zulässt, mit Mitteln erstellt wird, die nur der Unterzeichner kontrolliert, jede nachträgliche Änderung der signierten Daten ersichtlich macht und auf einem qualifizierten Zertifikat beruht.

Ein qualifiziertes Zertifikat kann nur von einem akkreditierten Zertifizierungsdiensteanbieter ausgestellt werden. Dabei gelten ganz besonders strenge Anforderungen hinsichtlich der Sicherheit der Schlüsselerstellung und der Organisation des Trustcenters. Die Einhaltung der gesetzlichen Vorschriften durch die Trustcenter wird in Deutschland ebenfalls von der Bundesnetzagentur kontrolliert.

## Public Key Verfahren

Digitale Signaturen basieren auf asymmetrischen Kryptosystemen und verwenden ein Schlüsselpaar, das aus einem privaten (geheimen) und einem öffentlichen (nicht geheimen) Signaturschlüssel besteht und sich gegenseitig ergänzt.

Daten, die mit dem einen Schlüssel verschlüsselt wurden, können nur mit dem anderen wieder geöffnet werden.

Beim Signieren wird der private Schlüssel verwendet. Dieser befindet sich auf dem Chip der Karte und lässt sich nicht auslesen. Die zu verarbeitenden Daten werden auf den Chip geladen, dort ver- oder entschlüsselt und wieder an den Computer übertragen.

Um den privaten Schlüssel zu benutzen, wird die richtige PIN benötigt, die zusätzliche Sicherheit gewährleistet. Die Signatur kann also nur vom Karteninhaber sein, denn nur er ist in Besitz von Karte und PIN.

Der öffentliche Schlüssel ist in ein Zertifikat integriert und steht jedermann zur Verfügung. Normalerweise kann dieser auch von Verzeichnisdiensten via LDAP oder HTTP abgerufen werden. Natürlich kann er auch per E-Mail versandt werden.

Um zu gewährleisten, dass dieses Zertifikat und somit der Schlüssel nicht gefälscht wurde, ist jedes Zertifikat vom Herausgeber signiert. Somit lässt sich überprüfen ob das Zertifikat von einer vertrauenswürdigen Stelle herausgegeben wurde.

Beim Prüfen der Signatur wird der öffentliche Schlüssel des Empfängers verwendet. Damit wird der verschlüsselte Hashwert des Herausgebers entschlüsselt und mit dem Hash des Dokumentes verglichen. Wenn beide Werte übereinstimmen wurde das Dokument nicht modifiziert.

Beim Signieren einer Datei wird ein Hashwert gebildet, der mit einem Fingerabdruck vergleichbar ist. Zwei verschiedene Dokumente können so nie denselben Hashwert haben. Der Hashwert wird nach dem RSA Verfahren unter Verwendung eines Schlüssels mit einer Länge von mindestens 1024 Bit (abhängig von der verwendeten Karte) verschlüsselt.

Die Verschlüsselung des Hashwerts findet auf dem Chipkartenprozessor statt, welcher kleinere Datenmengen verarbeiten kann. So wird sichergestellt, dass der private Schlüssel die Karte nicht verlässt. Der verschlüsselte Hash wird anschließend wieder an den Computer zurückgeschickt und in das zu signierende Dokument eingebaut. Vorher muss der private Schlüssel durch die richtige PIN (Personal Identification Number) freigegeben werden.

## 6. Language.ini

### Aloaha Übersetzung / Software-Lokalisierung

Neuste Produkte von Aloaha lokalisieren und übersetzen verwendete Zeichenfolgen (Strings) völlig automatisch. Die Zeichenfolgen werden als ini-Dateien gespeichert, um dem Anwender zu ermöglichen, sie zu ändern oder in eine andere Sprachen zu übersetzen, ohne den Aloaha-Code ändern zu müssen.

### Übersetzungs Mechanismus

- Beim Start des Aloaha-PDF-Multisignator werden die Spracheinstellungen in der language.ini überprüft. Sollte diese Datei nicht existieren, fragt das Programm folgende Pfade ab:
  - HKCU\Software\Aloaha\language
  - HKLM\Software\Aloaha\language
  - Die Betriebssystem Anwendersprache
- Basierend auf der "LanguageID" wird der Aloaha-PDF-Multisignator die UserLanguage\_<ID>.ini für die Übersetzung der Zeichenfolge abfragen. Wenn diese Datei nicht die richtige Übersetzung nicht enthält, fragt der Aloaha-PDF-Multisignator die Language\_<ID>.ini ab.
- Die Datei Language\_<ID>.ini wird durch jede(n) Neustart / Erweiterung (Update) überschrieben. Im Falle dass ein Benutzer Zeichenfolgen modifizieren möchte, wird darauf hingewiesen, die UserLanguage\_<ID>.ini zu verwenden.

### Language.ini

Das Profil [Abbildung] weist eine Sprache an, sich in einer anderen abzubilden . Zum Beispiel 410=409 würde bedeuten, englische Sprache (409) auf italienischen (410) Systemen zu verwenden.

Das Profil [languageID] definiert welche ini Dateien gegenwärtig zu verwenden sind.

### Übersetzungs-Dateien

Zuerst wird die Aloaha UserLanguage\_<ID> für die Übersetzung abgefragt. Sollte keine Übersetzung gefunden werden, wird als nächster Schritt die Language\_<ID> für die Übersetzung abgefragt.

Wenn ein Benutzer Zeichenfolgen ändern möchte, wird empfohlen, die Änderungen in UserLanguage\_<ID>.ini durchzuführen, da die Language\_<ID>.ini mit jedem Neustart/Upgrade überschrieben wird.

Es ist auch möglich, Registrierungsschlüssel HKLM\Software\Aloaha\pdf\WriteMissing auf 1 zu setzen. In diesem Fall wird der Aloaha-PDF-Multisignator alle Übersetzungsprobleme in der MissedLanguage\_<ID>.ini protokollieren. Es kann sehr nützlich sein, dass Zeichenfolgen für andere Sprachen / Umgebungen übersetzt werden.

## 7. Aloaha Signatur-Service

### Aloaha Signatur-Service

Der Aloaha Multisignator verfügt über einen Windows-spezifischen Service zum Signieren von PDF Dateien und zum Erzeugen von PKCS#7 Signaturen. Über CLI (command line interface) erhält man Zugriff zum Aloaha Signatur-Service.

Der Aloaha Signatur-Service wurde für Mehrfachsignaturenkarten optimiert. Wir empfehlen einen Kartenleser mit Display (Klasse III) für die PIN-Eingabe. Andere Kartenleser mit PIN Pad sind ebenfalls möglich, sofern sie eine Signalfunktion vor dem Start der PIN-Eingabe haben (z.B. Warnung durch einen Signalton).

Die Benutzung des Aloaha Signatur-Service ist sehr einfach. Benutzen Sie hierfür ACS.exe, die Sie im Aloaha-Installations-Ordner (<program files>\wrocklage) finden können.

Die Syntax der ACS-Befehlszeile ist sehr leistungsstark. Sollten Sie einen benötigten Befehl nicht finden, zögern Sie bitte nicht den Support unter: [info@aloaha.com](mailto:info@aloaha.com) anzufordern.

Weitere Informationen zum Aloaha ACS (command line signer) finden Sie hier.

### Info

Mit dem Befehl "Info" können Sie sich angeschlossene Kartenleser, eingeführte Karten und dort enthaltene Zertifikate anzeigen lassen. Wir empfehlen Ihnen den Befehl "Info" immer dann aufzurufen, wenn Sie Karten einführen, die dem System noch nicht bekannt sind.

Folgend sehen Sie ein Ausgabe-Beispiel des Info-Befehles:

```
C:\program files\wrocklage>acs -info
ReaderCount:4
0:OMNIKEY CardMan 3821 0
1:OMNIKEY CardMan 5x21 0
2:OMNIKEY CardMan 5x21-CL 0
3:SCM Microsystems Inc. SPRx32 USB Smart Card Reader 0

Reader:0,0,-1,0,-1,-1
Reader:1,0,-1,0,-1,-1
1,0)aloaha_b564d11f02d43f43daf5ecc2a882d65d73276b25
1,1)aloaha_dac91f79cb9d3642e6b1b0a5c5f5f565ac9e7a4e

Reader:2,0,-1,0,-1,-1
Reader:3,0,-1,0,-1,-1
3,0)aloaha_19bc2dd8432df733ff381722bcd183da2e1fff2c
3,1)aloaha_6e02cc5647e15114c3f03093d04ef4626dfd7199
```

Das oben angeführte Beispiel listet 4 angeschlossene Kartenleser (Reader) auf. Kartenleser 1 und 3 enthalten jeweils eine Smartkarte mit je 2 Zertifikaten.

## Open

Der Aloaha Signatur-Service wurde speziell für Mehrfachsignaturenkarten entwickelt. Solche Karten benötigen keinen PIN für jede einzelne Krypto-Operation. Z.B. ist es möglich eine Karte für eine Vielzahl von Signaturen oder für eine bestimmte Zeitdauer zu aktivieren.

```
C:\program files\wrocklage>acs -open:3,0 -maxtime:10 -maxsignatures:10
```

```
0:3,0,1,9,10|SCM Microsystems Inc. SPRx32 USB Smart Card Reader 0,7148
```

Die Zahlen in den Befehlsausgaben haben folgende Bedeutung:

0: OK  
3,0: Kartenleser 3, Zertifikat 0  
1,9: 1 Datei signiert, 9 Signaturen übrig  
(1 Signatur mit 00 Bytes wird benötigt, um die Karte zu öffnen)  
10: 10 Minuten sind noch übrig  
7148: Prozess-ID des Signatur-Service

## Sign PDF

Durch den Befehl `-oop -x:p` übergibt das ACS einen Signaturenjob an den Aloaha Service Signer. Die Option `-o` weist das ACS an, so lange zu warten, bis die Signatur übernommen wurde und die signierte Datei in die vorher definierte Datei zu speichern.

```
C:\program files\wrocklage>acs -oop -x:p -u:3,0 -sha2  
-i:c:\test.pdf -o:c:\signedpdf.pdf
```

Signed file: c:\signedpdf.pdf

`-oop -x:p` weist den Service an, eine PDF Signatur zu übernehmen  
`-sha2` erzwingt eine SHA256 Signatur  
`-u:3,0` legt fest, Kartenleser 3, Zertifikat 0 zu gebrauchen  
`-i` definiert die Input Datei  
`-o` warten und speichern der Output-Datei

## Create PKCS#7

```
C:\program files\wrocklage>acs -oop -x:a -u:3,0 -i:c:\test.pdf  
-o:c:\signedpdf.p7m
```

Signed file: c:\signedpdf.p7m

```
C:\program files\wrocklage>acs -oop -x:d -u:3,0 -i:c:\test.pdf  
-o:c:\signedpdf.p7s
```

Signed file: c:\signedpdf.p7s

`-oop -x:a`: erzeugt eine attached PKCS#7 Signatur  
`-oop -x:d`: erzeugt eine detached PKCS#7 Signatur

`-u:3,0`: benutzt Kartenleser 3, Zertifikat 0  
`-i`: Input Datei  
`-o`: Output Datei

## Reader status

Der Befehl "Reader Status" dient dazu zu prüfen, wieviele Signaturen oder wieviel Zeit noch übrig sind.

```
C:\program files\wrocklage>acs -readerstatus:3  
0:3,0,2,8,9|SCM Microsystems Inc. SPRx32 USB Smart Card Reader 0,7148
```

```
0: OK  
3,0: Kartenleser 3, Zertifikat 0 unbenutzt  
2: 2 Signaturen übernommen  
8: 8 Signaturen übrig  
9: 9 Minuten übrig  
7148: Prozess-ID des Signatur-Service
```

## Close

Der Befehl "Close" wird dazu benutzt, einen aktiven Kartenleser/Karte zu schließen.

```
C:\program files\wrocklage>acs -close:3,0  
0:OK
```

## 8. Aloaha Commandline Signer (ACS)

Informationen zum Aloaha Commandline Signator finden Sie hier:

[Aloaha Command Line Signator](#)

## 9. CryptoAPI

Das Cryptographic Application Programming Interface (auch bekannt unter Crypto API, Microsoft Cryptography API oder einfach nur CAPI), nachfolgend API oder CAPI genannt, ist ein API welches im Microsoft Windows Betriebssystem eingebunden ist, um Entwicklern den sicheren Gebrauch von Kryptographie-Modulen zu ermöglichen.

Crypto-API unterstützt sowohl symmetrische als auch allgemeine Kryptographie. Es schließt sowohl Funktionalitäten zum Ver- und Entschlüsseln als auch Beglaubigungen für Digitalzertifikate ein.

Crypto API wird durch das auf dem System installierten Aloaha CSP ergänzt. CSPs sind Module, welche die Verschlüsselung und Entzifferung von Daten durch kryptografische Funktionen ermöglichen. Sie sind weiterhin für die Kommunikation zwischen Smartcards und dem Windows Betriebssystem verantwortlich.

## 10. Technische Informationen

### Signaturstandards

PDF Signatur (signierte PDF Dokumente)  
EML Signatur (PDF Anhänge von angehängten eMail Dokumenten)  
PKCS#7 detached Signatur (beliebige Dokumente)  
PKCS#7 enveloped Signatur (beliebige Dokumente)  
Zeitstempel gemäß RFC 3161  
S/Mime V3 (signierte E-Mails)

### Aloaha Commandline Signer (ACS) integriert

### Massensignatur/Stapelsignatur

Fortgeschrittene & qualifizierte Massensignatur paralleler Betrieb mehrfacher Signaturkarten möglich

### Archivierung

Anbindung an beliebige Archivsysteme

### Management

Konfiguration über komfortable Windows Oberfläche

### Signaturprüfung

Zentrale automatische Signaturprüfung  
Certificate Revocation List (CRL) &  
OCSP (Online Certificate Status Protocol) Prüfungen  
Prüfergebnis kann mitarchiviert werden  
Prüfergebnis in XML als XAdES möglich

### Kompatibilität

Integration in alle Buchhaltungssysteme ist gegeben

### Integration

SMTP (E-Mail Schnittstelle)  
WebDAV  
Hotfolder (Dateien werden in einen Ordner kopiert und von dort verarbeitet)  
POP3 Downloader/Mailbox polling

### Secure Pin Caching

#### Systemvoraussetzungen:

Windows 2000, Windows XP, Windows 2003 oder Windows Vista. Keine Softwarepakete von Drittanbietern notwendig. Greift problemlos auf die Infrastruktur jedes Kartenanbieters zu, z. B. CAs, Zertifikate, CRLs, OCSP Responder, SmartCards usw.

Aktuell nativ unterstützte Karten (für diese Karten benötigen Sie keinen Kartentreiber/CSP) (Stand: März 2008):

SECCOS (S-Trust SparkassenCard), TCOS (TeleSec), D-Trust, Arztausweis (HBA), Apotheker Karte, Krankenversicherungskarte (eGK), Belpic, a-sign premium (Bürgerkarte), TC Trustcenter QSign, GS1 Schweiz und SiCryptbasierte Karten.

Wir arbeiten ständig an der Unterstützung weiterer Kartentypen! Kontaktieren Sie uns, wenn Ihre Karte noch nicht dabei sein sollte.

## 11. FAQ Multisignator

Durch drücken der F1 Taste werden Sie direkt zur Aloaha Online Hilfe im Internet weitergeleitet. Falls Sie auch Fragen zu anderen Aloaha Produkten haben, werden Sie hier sicher Antworten finden.

### Wie kann ich definieren, an die welche E-Mail-Adresse Aloaha das unterzeichnete Dokument schicken soll?

Es gibt zwei Möglichkeiten.

1. Sie können die Aloaha eingebetteten Kommandos wie emailto verwenden. Aloaha liest die Befehle des Dokumentes selbst. Der Befehl emailto definiert den / die Empfänger.
2. Sie können Unterverzeichnisse in Ihrem konfigurierten inputfolder anlegen. Wenn der Name des Unterverzeichnisses eine E-Mail-Adresse ist, wird Aloaha das als emailto verwenden. Starten Sie den Multisignator nach dem  
Anlegen neuer Unterverzeichnisse neu.

Eine Kombination von 1 und 2 ist möglich. Zum Beispiel können Sie das Unterverzeichnis-Funktionalität verwenden, um eine E-Mail zu definieren, zu der immer als Empfänger verwendet wird. Zusätzliche Empfänger werden dann über 1 (eingebettete Kommandos) definiert.

### Ist es möglich E-Mails zu signieren?

Mit dem Aloaha Multisignator es ist möglich, in E-Mail eingebettete PDF-Dokumente zu signieren. Wenn Sie \*.eml Dateien in einen der konfigurierten Eingangsordner verschieben, unterzeichnet Aloaha alle PDF-Dokumente die in eml Dateien eingebettet sind digital.

Es ist auch möglich, den integrierten POP3 downloader zu verwenden, um E-Mails von einem externen POP3 Account herunterzuladen und sie in den Dropfolder zu verschieben.

### Kann Aloaha \*.eml Dateien mit SMTP versenden?

Ja, wenn Mailversand aktiviert ist, verschickt Aloaha die E-Mail über den konfigurierten SMTP Server automatisch.

Im Falle dass das Eingangsverzeichnis die Form einer E-Mail-Adresse hat, schreibt Aloaha die Empfänger-Adresse automatisch um, so dass die Empfänger Adresse die Ordnernamen vergleicht.

Sollte die E-Mail Zustellung über SMTP scheitern, wird Aloaha die E-Mail dem lokalen IIS Verzeichnis zustellen. Sollte dies auch scheitern, wird die \*.eml Datei im Ordner der fehlgeschlagener Zustellung gespeichert.

### Kann ich verschiedene Profile laden?

Ja, standardmäßig speichert Aloaha die Einstellungen in der Datei MultiSignator.ini. Pro Befehlszeile können Sie jede andere Konfigurationsdatei öffnen.

Zum Beispiel: AloahaMultiSignator.exe AlternativeSettings.ini

### Kann ich verschiedene Zertifikate pro dropfolder konfigurieren?

Ja, nachdem Sie den Ordner konfiguriert haben, klicken Sie mit der rechten Maustaste auf ihn und wählen Einstellungen wie POP3, Unterschrift usw.

### Wie konfiguriere ich den POP3 Downloader?

Der POP3 Downloader wird pro Hotfolder konfiguriert. Das bedeutet, dass Sie auf den konfigurierten Hotfolder mit der rechten Maustaste klicken und POP3 wählen, um den POP3 Downloader für diesen Ordner zu konfigurieren.

### **Ich verstehe die Optionen des POP3 Downloader Dialog nicht.**

POP3Frequency (Sekunden) definiert, wie oft das POP3 Modul aufgerufen wird.

Max. POP3 Prozesse definiert, wie viele POP3-Prozesse gestartet werden.

POP3Frequenz definiert, wie häufig einem POP3 Server erlaubt wird, in den Modus "Verbinden" gesetzt zu werden.

Max Downloads definiert, wie viele E-Mails aus dem Posteingang heruntergeladen werden.

Postempfänger definiert die Zieladresse. Diesem Empfänger werden die Dokumente geschickt.

Wenn CC Absender aktiviert ist, wird jede CC E-Mail dem ursprünglichen Absender ebenfalls zugestellt.

### **Ich habe den POP3 Downloader konfiguriert, es werden aber keine E-Mails heruntergeladen**

Um Ressourcen zu sparen, wird Aloaha das POP3 Modul NUR aufrufen, wenn alle Dropfolder leer sind.

### **Wie kann ich sicherstellen, dass keine E-Mails verloren gehen, falls ich Probleme mit meiner Netzwerkkonnektivität habe?**

Standardmäßig verschickt Aloaha die E-Mails über SMTP. Sollte dies durch Netzwerkprobleme scheitern, versucht Aloaha Mails dem lokalen IIS Verzeichnis zu übergeben. Sobald wieder ein Netzwerk vorhanden ist, wird IIS das Mail zustellen. Aus diesem Grund wird empfohlen (aber nicht erforderlich) Aloaha auf einer Maschine mit einem korrekt konfigurierten IIS SMTP Server laufen zu lassen.

### **Wie kann ich herausfinden, warum Aloaha keine Mails von meinem Briefkasten herunterladen kann?**

Aloaha schreibt das letzte Problem in die Datei Multisignator.ini.

### **Ist es möglich, die unterzeichneten Dokumente zu einer webbasierten Dokumentenbibliothek hochzuladen?**

Ja, konfigurieren Sie die URL als Zielordner. Aloaha lädt die unterzeichneten Dokumente automatisch hoch.

### **Ist es möglich, Dokumente direkt am C-Prompt zu signieren?**

Ja, allerdings benötigen Sie dazu den Aloaha CommandLineSigner (CLS).

Weitere Informationen dazu finden Sie hier:

<http://www.aloaha.com/software-development/aloaha-commandline-signer-cls.php>

### **Wie rufe ich die Hilfe auf?**

Drücken Sie F1 oder führen Sie einen Doppelklick auf das Aloaha Logo aus.

### **Welche Smartcards werden empfohlen?**

Alle Aloaha unterstützten Smartcards und auch Software Zertifikate funktionieren. Für die Massensignatur werden aber sogenannte Multisign Karten empfohlen.

### **Unterstützt der Multisignator auch WebDAV?**

Ja, dazu tragen Sie einfach in "Ausgabe Verzeichnis" eine http Adresse ein. Zum Beispiel <http://YourExchangeServer.tld/public/rechnungen>

### **Ist es möglich spezielle Konfigurationen zu laden?**

Ja, alle Einstellungen werden in der Datei MultiSignator.ini gespeichert. Sie können verschiedene INI Dateien erstellen und diese direkt laden. Dazu starten Sie bitte den Multisignator vom Command Prompt und geben als Parameter die zu ladene INI Datei an.

### Welche zusätzlichen INI Parameter werden unterstützt?

Mit den folgenden Parametern können Sie in der Multisignator.ini Einstellungen per Verzeichnis vornehmen:

Location  
Reason  
PicPath  
SigContent  
px1  
py1  
px2  
py2

### Gibt es ein Logfile bzw. wie kann ich große Dateien (200-800 MB) signieren?

PDF Dateien werden beim Signieren in den Speicher geladen und technisch normiert. Bei derart großen Dateien schlägt das fehl.

Es gibt einen Registry key, mit dem das Verhalten ausgeschaltet wird:

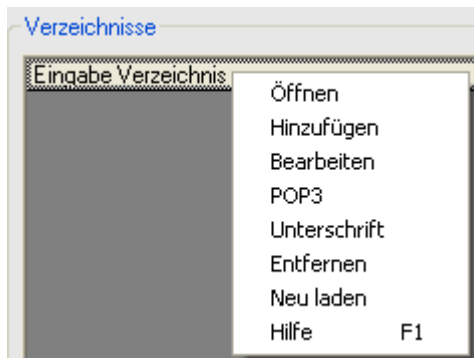
```
HKLM\Software\Aloaha\pdf\minSignature = 1
```

Setzen Sie diesen Key, dann sollte es funktionieren.

**Wenn Sie weitere Fragen haben, zögern Sie nicht, sich mit uns in Verbindung zu setzen.**

## 12. Tipps und Tricks

Sämtliche Einstellungen können auch durch Klick mit der rechten Maustaste auf das Feld Verzeichnisse aufgerufen werden.



Durch drücken der F1 Taste werden Sie direkt zur Aloaha Online Hilfe im Internet weitergeleitet. Falls Sie auch Fragen zu anderen Aloaha Produkten haben, werden Sie hier sicher Antworten finden.

# Index

## - A -

Aktiviere Mailer 23  
Aloaha Commandline Signer 31  
Aloaha Signatur-Service 28  
Anwendung 5  
Archivierung 32  
Art des Zertifikats 14  
Ausgabe Verzeichnis 23  
Automailer 20

## - B -

Bearbeiten 23  
Benutzer 24  
Bild Unterschrift 14

## - C -

Close 28  
Commandline Signer 32  
Create PKCS#7 28  
CryptoAPI 31

## - D -

Digital Signieren 25  
Digitale Unterschrift 14  
Drop Verzeichnis 24

## - E -

Eingabe Verzeichnis 23  
Einleitung 4  
Einstellungen 13  
Entfernen 23  
Erscheinung der Signatur 14

## - F -

FAQ Multisignator 33

## - G -

Gesetzliche Regelungen 25

Globale Einstellungen 21

## - H -

Hinzufügen 23

## - I -

Inkrementelle Signatur 14  
Installation 8, 9  
Integration 32

## - K -

Kompatibilität 32  
Konfiguration 12

## - L -

Language.ini 27

## - M -

Mail Empfänger 24  
Mailserver 20  
Management 32  
Massensignatur/Stapelsignatur 32  
Max. Downloads 24  
Max. Pop3 Prozesse 24

## - N -

Neu laden 23

## - O -

Open 28  
Original Verzeichnis 23

## - P -

Passwort 24  
POP3 Einstellungen 24  
Pop3 Frequenz 24  
Port 24  
Position der Signatur 21  
Public Key Verfahren 25

**- R -**

Reader status 28

**- S -**

Secure Pin Caching 32

Sender in Kopie 24

Server 24

Sign PDF 28

Signaturprüfung 32

Signatur-Service 28

Signaturstandards 32

Standard 20

Systemvoraussetzungen 8, 32

**- T -**

Technische Informationen 32

Text Unterschrift 14

Tipps und Tricks 36

**- U -**

Übersetzungs Mechanismus 27

Übersetzungs-Dateien 27

Unterschreiben 23

**- V -**

Verzeichnis fehlgeschlagener Dokumente 21

Verzeichnis Picker 23

Verzeichnisse 20

**- Z -**

Zeitstempel 14

Zertifikat auswählen 14

Zertifikatquelle 14

Zweck der Signatur 14