Aloaha Sign!

Aloaha Sign!

Printed: Dezember 2009

Inhalt

1. Einleitung

Aloaha Sign!

Diese Software wurde von Aloaha entwickelt um digitale Unterschriften anzeigen und überprüfen zu können. Zusätzlich kann jede Datei digital signiert werden.

Zur Überprüfung von digitalen Signaturen werden unterstützt:

- PKCS7
- XMLDSIG
- PDF
- P7M / SMIME

Das Signieren von Dateien wird in folgenden Formaten untertsützt:

- PKCS7
- XMLDSIG
- PDF (wenn der Aloaha Signator auf dem System installiert ist)
- P7M / SMIME

Selbstverständlich werden viele Signaturkarten nativ unterstützt.

Weitere Aloaha Produkte:

- Aloaha PDF Suite - Erstellt Ihre PDF-Dateien. Mit einem sehr hohen Funktionsumfang ist diese Suite die umfangreichste PDF-Software am Markt. Unterstützt digitale PDF-Signaturen mittels Smartkarten und vieles mehr.
- Aloaha PDF Saver - Sie können Formulardaten in Ihre PDF-Formulare schreiben und abspeichern. Sie benötigen keine Vollversion von Adobe Acrobat und sparen sich so die Lizenzgebühren.
- Aloaha Crypto Service Provider – Benutzen Sie Ihre Qualifizierte Signaturkarte um Dokumente und E-Mails in Standardsoftware wie Microsoft Outlook oder in der Adobe Acrobat Vollversion digital zu signieren.

2. Installation

Installationsvoraussetzungen

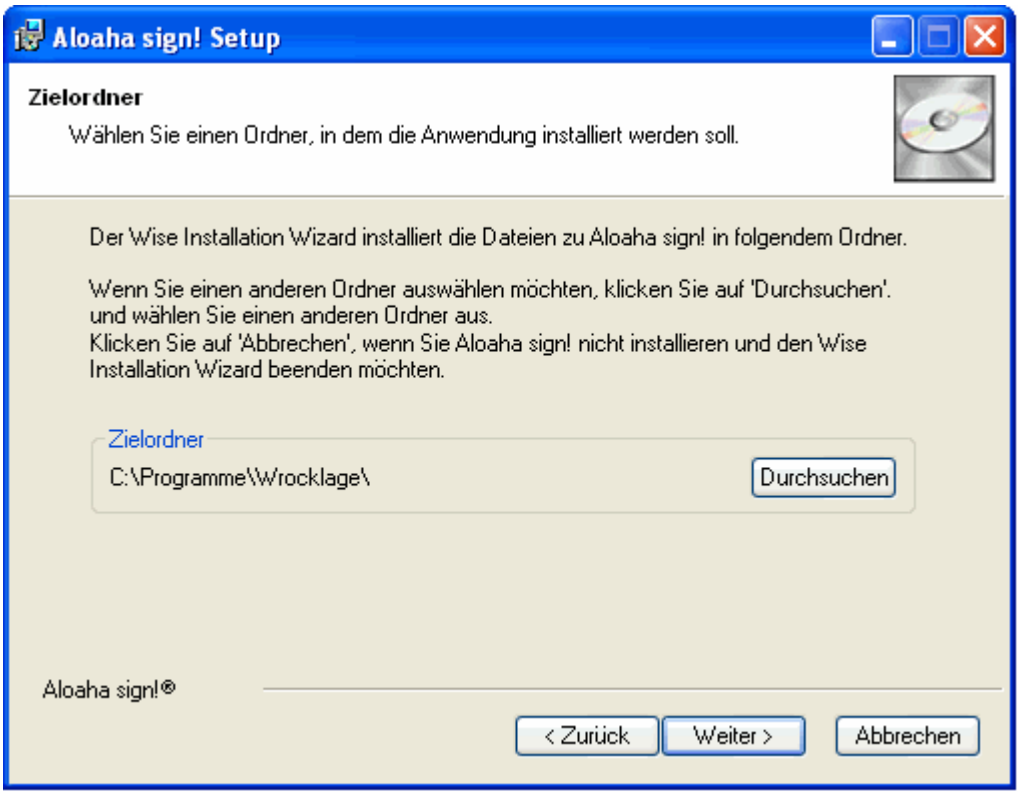
- Windows 2000/3/8
- Windows XP (Service Pack 3 empfohlen, aber nicht zwingend erforderlich)
- Windows Vista
- Windows 7

Um Aloaha Sign zu installieren, starten Sie die Installationsdatei (*aloaha_sign_setup.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".

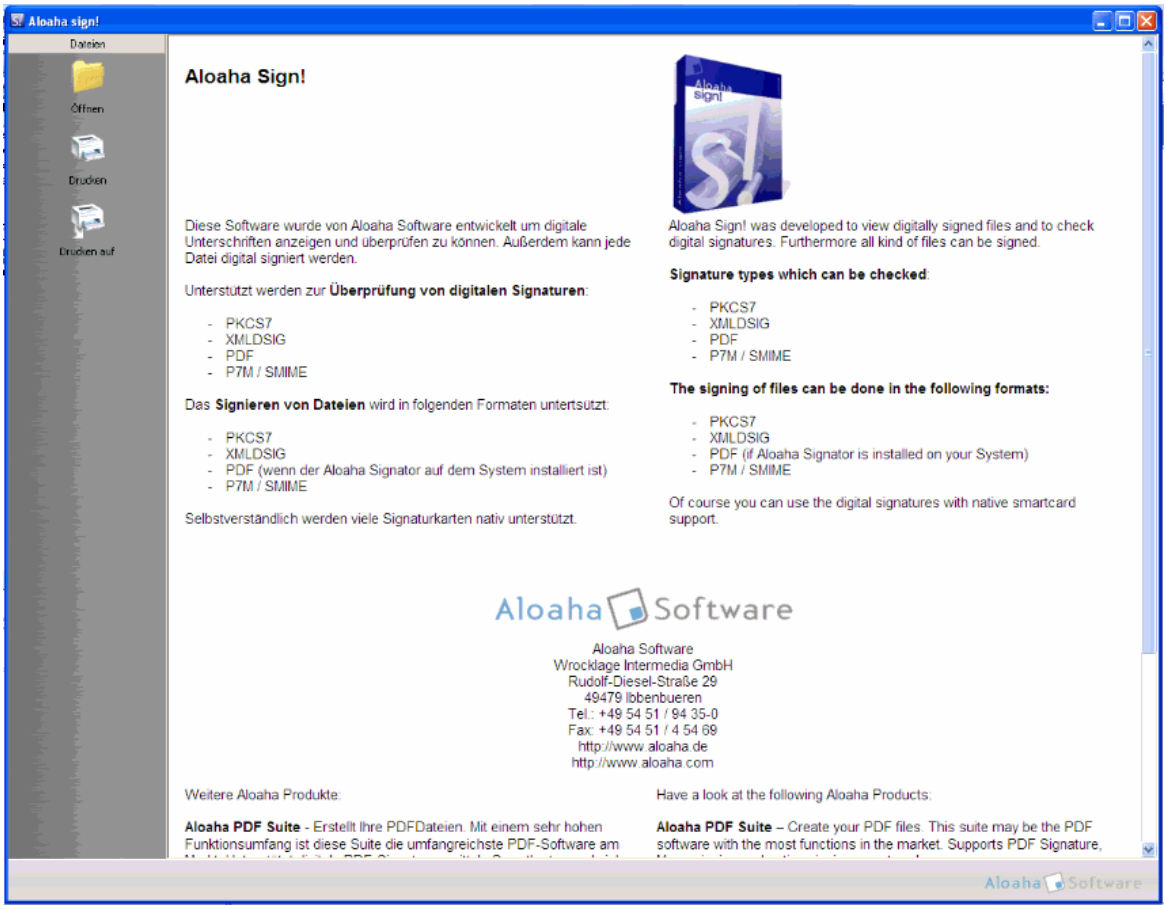


Hinweis: Der Standard-Installationspfad kann meistens akzeptiert werden.

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

Um Aloaha Sign zu starten, wählen Sie das Programm Aloaha Sign im Windows Startmenü:
Start>Alle Programme>Aloaha>Aloaha Sign!

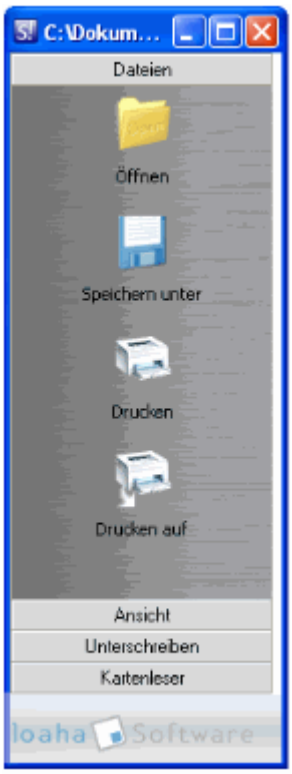


Es stehen nun folgende Optionen zu Verfügung:

- Datei
- Ansicht
- Signieren
- Kartenleser

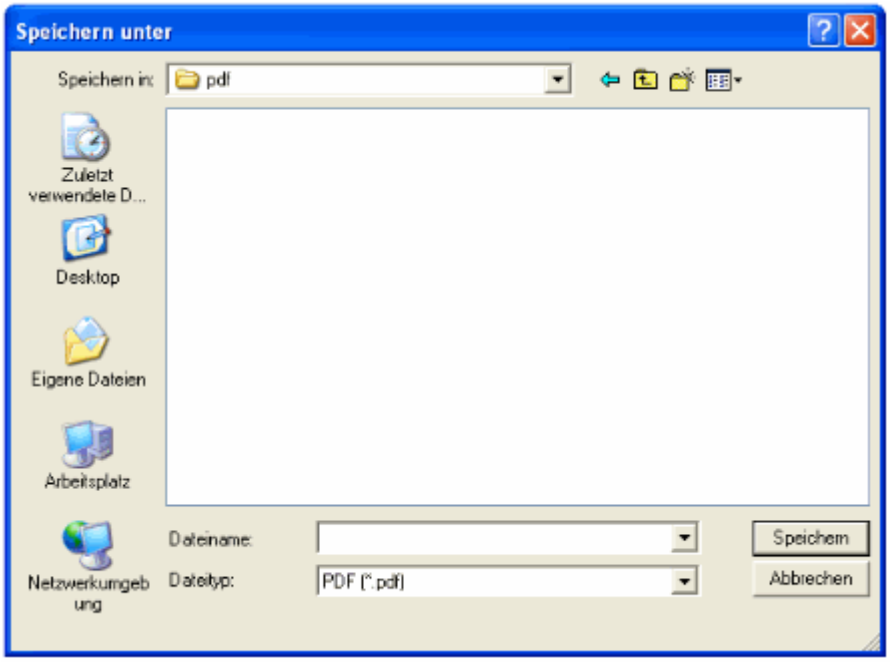
3.1 Öffnen

Sollten Sie ein verschlüsseltes Dokument öffnen bei dem eine digitale ID verwendet wurde, ist es zwingend erforderlich, dass Ihre digitale ID korrekt installiert ist, ggf. wenden Sie sich an den Verfasser des Dokumentes.
Steht Ihnen keine digitale ID zu Verfügung, kann das Dokument nicht geöffnet werden.



3.2 Speichern unter

Wenn Sie eine signierte PDF Datei abspeichern möchten, wählen Sie "Speichern unter" in dem von Ihnen gewählten Verzeichnis.

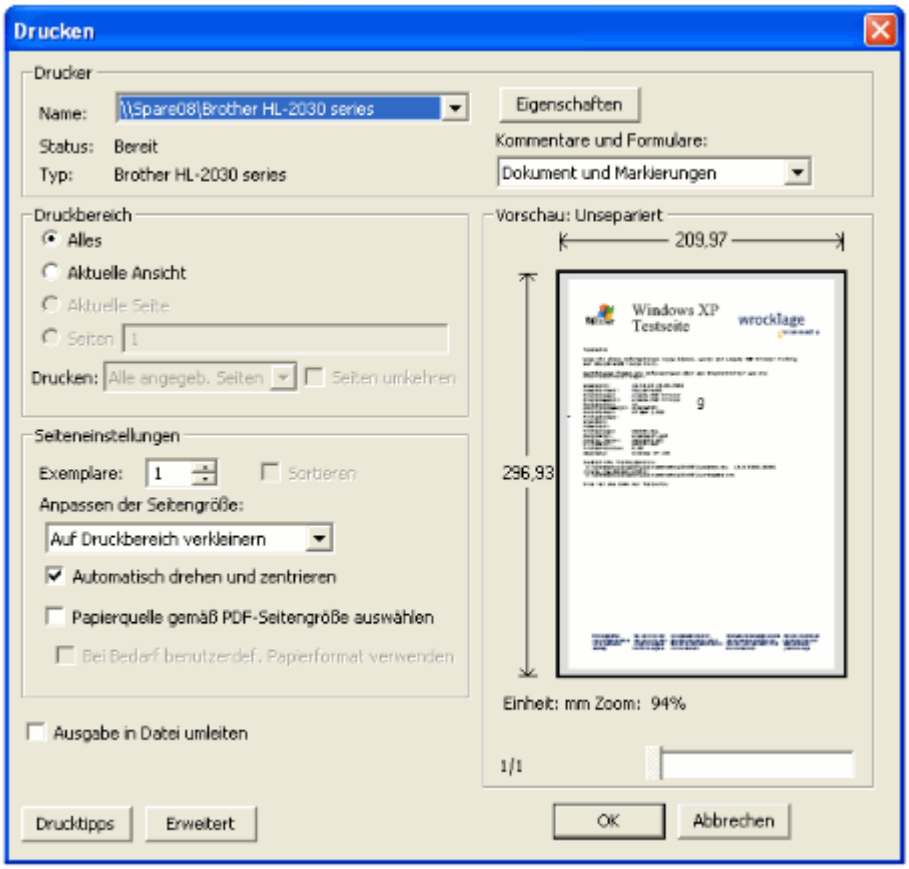


3.3 Drucken

Drucken:

Das zu druckende Dokument wird direkt an den installierten Drucker gesendet.

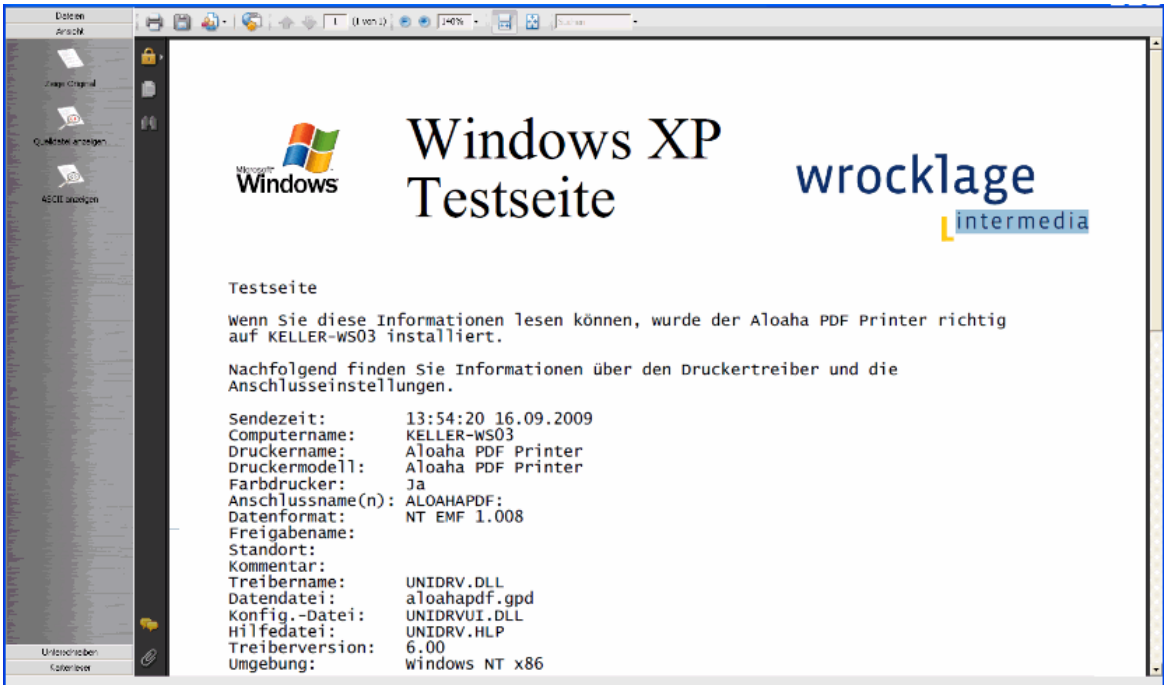
Drucken auf:
Für diese Druckoption stehen alle im System installierten Drucker zu Verfügung.
Es kann der Standarddrucker aber auch jeder andere angewählt werden, um das Dokument auszugeben.



3.4 Ansicht

Im Menü Ansicht haben Sie folgende Möglichkeiten, sich Dokumente anzeigen zu lassen:

- **Zeige Original** bedeutet, dass wenn das Originaldokument in MS Word erstellt wurde, dieses zur Ansicht ebenfalls wieder in MS word geöffnet wird!
- **Quelldatei anzeigen** bedeutet, dass der entsprechende Quelltext zu den jeweiligen Dokument angezeigt wird.
- **ASCII anzeigen** bedeutet, dass das entsprechende Dokument im ASCII Format angezeigt wird.



3.5 Unterschreiben

Mit Aloaha Sign! haben Sie die Möglichkeit, Dokumente zu signieren (unterschreiben).
Hier stehen folgende Unterschriftsformate zu Verfügung:

- D2D Unterschrift
- P7M Unterschrift
- XML Unterschrift
- PKC#7 Unterschrift
- PDF Unterschrift

Weitere Informationen hierzu finden Sie in der Rubrik **"Digital Signieren / Signaturprüfung"**

3.6 Digital Signieren / Signaturprüfung

Dateien elektronisch unterschreiben

Mit Aloaha Sign! können Sie 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 Aloaha Sign! 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 Paragrafen 14 Abs. 3 Umsatzsteuergesetz dar.

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 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.

3.6.1 Signaturvorgang

Diese Software wurde von Aloaha Software entwickelt um digitale Unterschriften anzeigen und ü berprüfen zu können. Außerdem kann jede Datei digital signiert werden.

Das Signieren von Dateien wird in folgenden Formaten unterstützt:

- PKCS7
- XMLDSIG
- PDF (wenn der Aloaha Signator auf dem System installiert ist)
- P7M / SMIME

Unterschreiben:

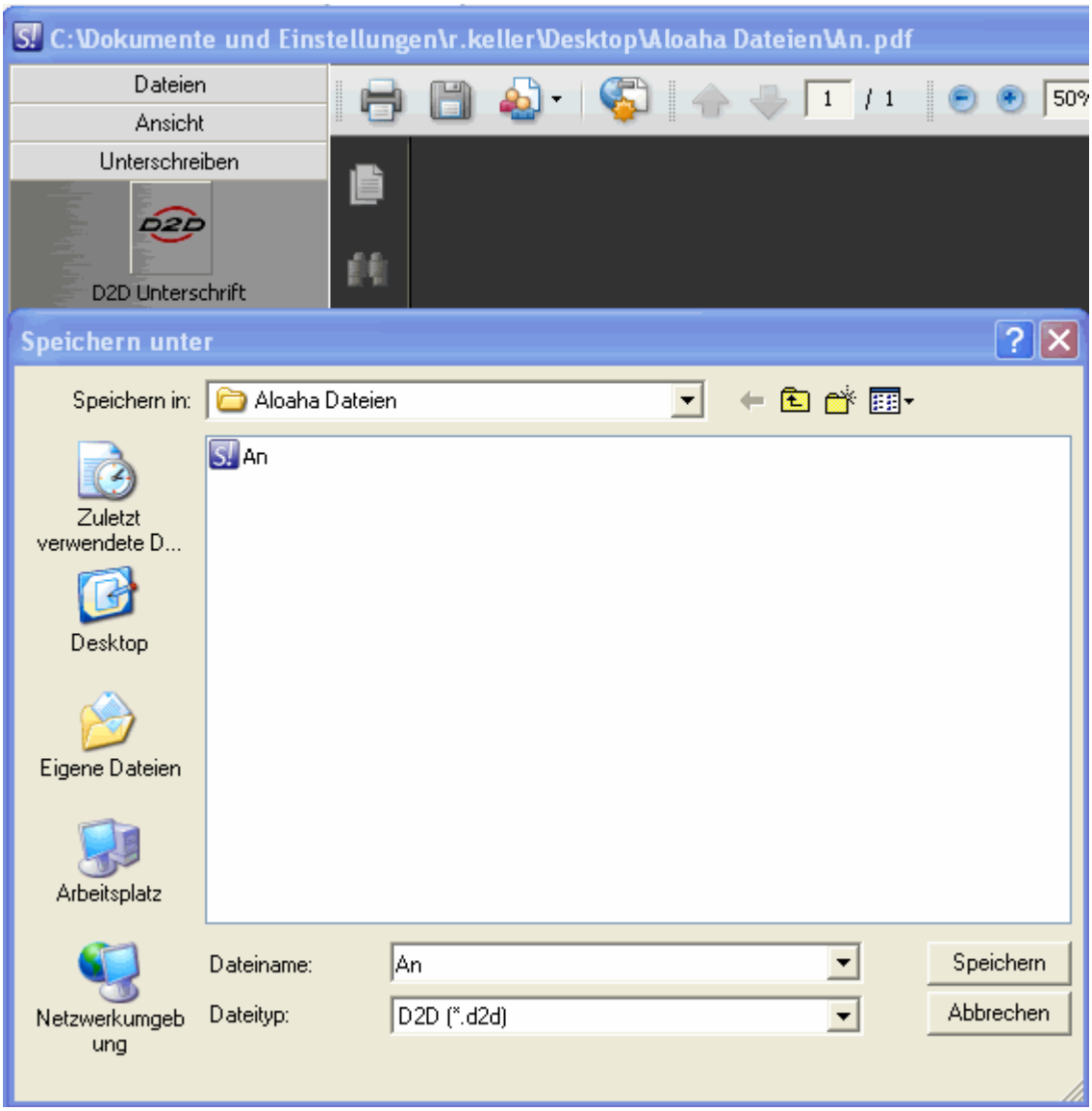
Mit Aloaha Sign! haben Sie die Möglichkeit, Dokumente zu unterschreiben.

Hier stehen folgende Unterschriftsformate zu Verfügung:

- D2D Unterschrift
- P7M Unterschrift
- XML Unterschrift
- PKC#7 Unterschrift
- PDF Unterschrift

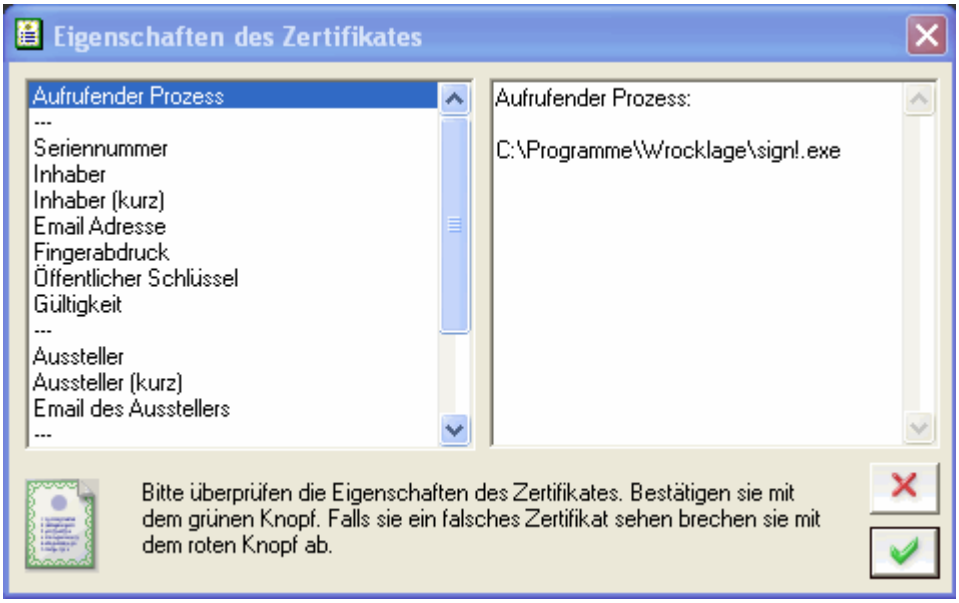
Signaturvorgang:

Wenn Sie ein geöffnetes Dokument signieren möchten, werden Sie zunächst nach dem Speicherort gefragt, an welchem das Dokument nach erfolgter Signatur gespeichert werden soll.



Nachdem Sie den Speicherort ausgewählt und den Dateinamen festgelegt haben, öffnet sich ein Fenster mit den "Eigenschaften des Zertifikates".

Bestätigen Sie das zu verwendende Zertifikat, indem Sie auf das Feld mit dem grünen Haken klicken.



Jetzt werden Sie zur Eingabe der dem Zertifikat zugeordneten PIN aufgefordert.
Geben Sie die entsprechende PIN ein und bestätigen Sie anschließend die Eingabe.

Im Anschluss an den Signaturvorgang wird das Dokument an dem von Ihnen gewählten Speicherort zu finden sein.

Hinweis: Eingebettete Dateien werden ebenfalls signiert.

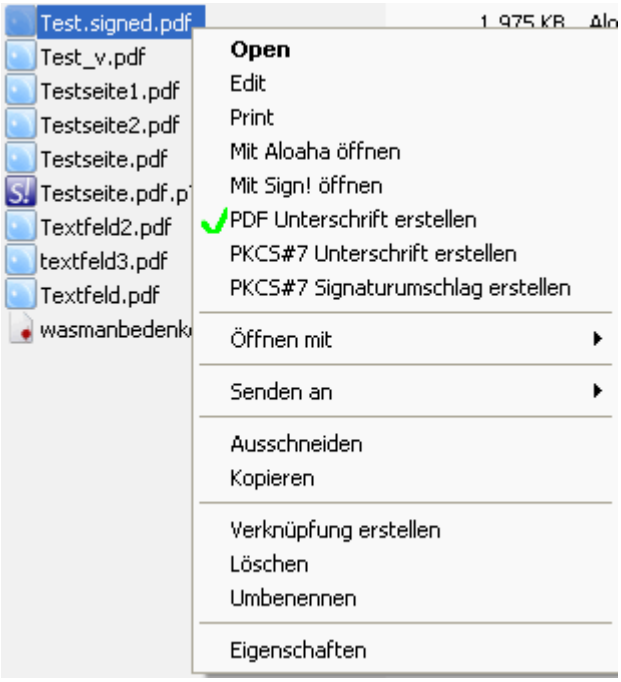
3.6.2 Signaturprüfung

Unterstützt werden zur Überprüfung von digitalen Signaturen:

- PKCS7
- XMLDSIG
- PDF
- P7M / SMIME

Um Aloaha Sign! in vollem Umfang nutzen zu können, ist es sinnvoll, die Aloaha PDF Suite oder den Aloaha Signator ebenfalls zu installieren.

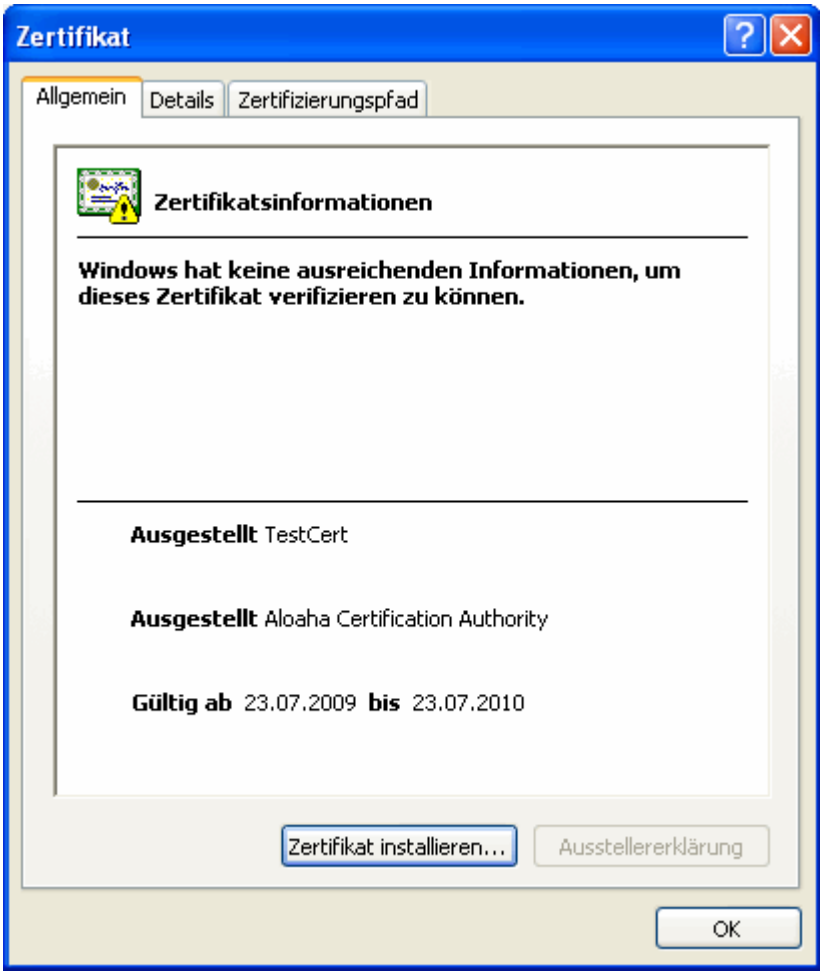
Möchten Sie die Unterschrift eines Dokumentes überprüfen oder ein Dokument, welches mit einer anderen Anwendung erstellt wurde öffnen, können Sie im Windows Explorer mit der rechten Maustaste die Datei auswählen und anschließend **mit Sign! öffnen**.



Anschließend werden Sie gefragt, ob Sie die Datei öffnen oder speichern wollen?

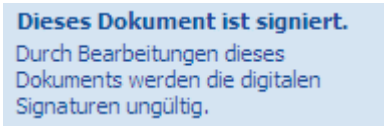
Wichtig: Ist die Datei nicht verschlüsselt / signiert, wird das Dokument in der Anwendung geöffnet, in welcher es erstellt wurde, obwohl Sie den Befehl "Öffnen" in Aloaha Sign! gewählt haben. Bei verschlüsselten / signierten PDF Dokumenten wird der Aloaha PDF Editor verwendet! Hier öffnet sich ein weiteres Fenster.

Vorher öffnet sich ein weiteres Fenster, um die dem Zertifikat zugeordneten Eigenschaften wie "Gültigkeit, Aussteller, etc." anzuzeigen.



Nachdem die Datei importiert wurde, wird sie durch den Aloaha PDF Editor die Datei angezeigt.

Werden signierte Dokumente nachträglich bearbeitet, verliert die Signatur ihre Gültigkeit.



3.7 Kartenleser

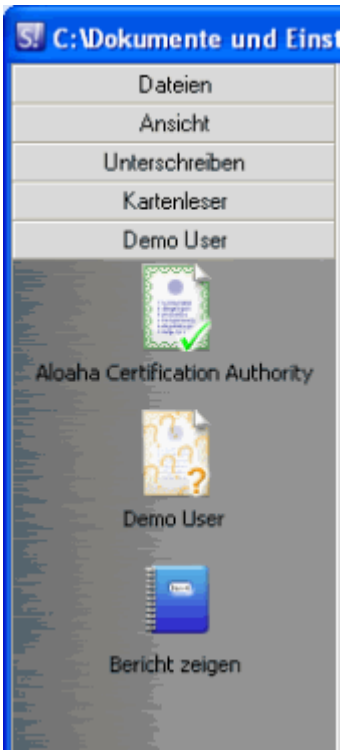
Im Menüpunkt Kartenleser können Sie sehen, ob und welche(r) Kartenleser mit dem System verbunden ist.

Durch einen Klick mit der rechten Maustaste auf das Kartenlesersymbol werden die Informationen der verwendeten

Signaturkarte angezeigt.

3.8 Zertifikatprüfung

Im Menüpunkt Zertifikatsprüfung finden Sie Informationen zu dem jeweiligen Zertifikat des jeweiligen Users.



Folgende Punkte stehen bei der Zertifikatsprüfung zu Verfügung:

Hier erhalten Sie Informationen über:

Alaoaha Certification Authority - Informationen zum aktuell verwendeten Zertifikat

Demo User - aktuell verwendete Karte im Kartenlesegerät

Bericht anzeigen - Anzeigen des Reports zur Signaturprüfung und der aktuell verwendeten Signatureinstellung.

3.9 Aloaha PDF Signature Bulk Validator

Der Aloaha PDF-Bulk Validator ist ein add-on für Aloaha-Sign!.

Gültige PDF-Dokumente werden in Unterverzeichnisse abgelegt.

Um ein ganzes Verzeichnis von PDF-Dokumenten gültig zu machen, starten Sie AloSiVal.exe <Directory>. Es ist WICHTIG, dass **<Directory>** mit einem Backslash endet!. **Beispiel**: **AloSiVal.exe C:\PDF**

Gültige Dokumente werden in Unterverzeichnisse unter **\ValidatedPDF** abgelegt. Unterverzeichnis können in **HKEY_LOCAL_MACHINE\SOFTWARE\Aloaha\Validator\TargetDir** konfiguriert werden.

PDF-Dokumente mit ungültiger Signatur werden in entsprechende Unterverzeichnisse sortiert. Solche Dokumente sind nach dem Signaturvorgang editiert worden.

Für jeden Status einer Signatur wird ein Bitmask angelegt, welches weiterhin als Verzeichnisname verwendet wird. In **HKEY_LOCAL_MACHINE\SOFTWARE\Aloaha\Validator** ist es möglich, die entsprechenden Verzeichnisse mit einem Namen in Klartext zu benennen.

Mögliche Bitmask Werte

- **IS NOT TIME VALID = &H1**

Dieses oder eines der Zertifikate in der Zertifikatkette ist zeitlich nicht gültig.

- **IS NOT TIME NESTED = &H2**

Zertifikate in der Kette sind zeitlich nicht richtig miteinander verschachtelt.

- **IS REVOKED = &H4**

Das Treuhandverhältnis für dieses oder eines der Zertifikate in der Zertifikatkette ist widerrufen worden.

- **NOT SIGNATURE VALID = &H8**

Das oder eines der Zertifikate in der Zertifikatkette haben keine gültige Unterschrift.

- **NOT VALID FOR USAGE = &H10**

Das Zertifikat- oder die Zertifikatkette ist für den vorgeschlagenen Gebrauch nicht gültig.

- **IS UNTRUSTED ROOT = &H20**

Das Zertifikat- oder die Zertifikatkette beruht auf einem nicht vertraulichen Ursprung.

- **REVOCATION STATUS UNKNOWN = &H40**

Der Widerrufsstatus des Zertifikats oder eines der Zertifikate in der Zertifikatkette sind unbekannt.

- **IS CYCLIC = &H80**

Eines der Zertifikate in der Kette wurde von einer Zertifikat-Autorität ausgegeben, die das ursprüngliche Zertifikat bescheinigt hatte.

- **INVALID EXTENSION = &H100**

Eines der Zertifikate hat eine Erweiterung, die nicht gültig ist.

- **INVALID POLICY CONSTRAINTS = &H200**

The certificate or one of the certificates in the certificate chain has a policy constraints extension, and one of the issued certificates has a disallowed policy mapping extension or does not have a required issuance policies extension.

- **INVALID BASIC CONSTRAINTS = &H400**

Das Zertifikat oder eines der Zertifikate in der Zertifikatkette haben eine grundlegende Einschränkungserweiterung und entweder das Zertifikat kann nicht verwendet werden, um andere Zertifikate auszugeben oder die Pfadlänge ist überschritten worden.

- **INVALID NAME CONSTRAINTS = &H800**

Das Zertifikat oder eines der Zertifikate in der Zertifikatkette haben eine Namenseinschränkungserweiterung, die ungültig ist.

- **HAS NOT SUPPORTED NAME CONSTRAINT = &H1000**

Das Zertifikat oder eines der Zertifikate in der Zertifikatkette haben eine Nameneinschränkungserweiterung, die nicht unterstützte Felder enthält. Die minimalen und maximalen Felder werden nicht unterstützt! So muss Minimum immer Null sein und Maximum fehlen. Nur UPN wird für einen anderen Namen unterstützt.

Die folgenden alternativen Namenswahlen werden nicht unterstützt:
- X400 Address
- EDI Party Name
- Registered Id

- **HAS NOT DEFINED NAME CONSTRAINT = &H2000**

Das Zertifikat oder eines der Zertifikate in der Zertifikatkette haben eine Namenseinschränkungserweiterung obwohl eine Namenseinschränkung für eine der Namenswahlen im Endzertifikat vermisst wird.

- **HAS NOT PERMITTED NAME CONSTRAINT = &H4000**

Das Zertifikat oder eines der Zertifikate in der Zertifikatkette haben eine Namenseinschränkungserweiterung obwohl es keine erlaubte Namenseinschränkung für Namenwahlen im Endzertifikat gibt.

- **HAS EXCLUDED NAME CONSTRAINT = &H8000**

Das Zertifikat oder eines der Zertifikate in der Zertifikatkette haben eine Namenseinschränkungserweiterung obwohl die Namenswahl im Endzertifikat ausführlich ausgeschlossen wird.

- **IS OFFLINE REVOCATION = &H1000000**

Der Widerrufsstatus des Zertifikats oder eines der Zertifikate in der Zertifikatkette sind entweder offline oder veraltet.

- **NO ISSUANCE CHAIN POLICY = &H2000000**

The end certificate does not have any resultant issuance policies, and one of the issuing CA certificates has a policy constraints extension requiring it.

- **IS PARTIAL CHAIN = &H10000**

Die Zertifikatkette ist nicht komplett.

- **CTL IS NOT TIME VALID = &H20000**

Ein zur Erstellung der Kette verwendeter CTL hat keine zeitliche Gültigkeit.

- **CTL IS NOT SIGNATURE VALID = &H40000**

Ein zur Erstellung der Kette verwendeter CTL hat keine gültige Unterschrift.

- **CTL IS NOT VALID FOR USAGE = &H80000**

Ein zur Erstellung der Kette verwendeter CTL ist für diesen Gebrauch ungültig.

Jeder mögliche Wert kann in Klartext in **HKEY_LOCAL_MACHINE\SOFTWARE\Aloaha\Validator** dargestellt werden.

3.10 FAQ

Kann ich, Aloaha Sign! verwenden, um eine digitale signatur auf PDF-Dokumente anzuwenden?

Sie brauchen eines der Aloaha PDF-Produkte, um Digitalunterschriften auf PDF-Dokumente anzuwenden. Aloaha Sign! wwurde entworfen, um NICHT PDF-Dokumente zu unterzeichnen.

Brauche ich einen CSP um eine Datei zu unterzeichnen?

Aloahas innovative Technologie unterstützt eine breite Reihe nativer Smartcards. Das bedeutet, dass kein CSP für solche Chipkarten erforderlich ist!

Welchen Typ von Unterschriften kann ich mit Aloaha Sign! erstellen?

Aloaha Sign! ist in der Lage p7m, PKCS#7 und XMLDSIG Signaturen zu erstellen.

Was ist eine p7m Datei?

Eine p7m Datei ist ein digital unterzeichneter elektronischer Umschlag, der die ursprüngliche Datei enthält. P7M wird auch s/Mime genannt.

Was ist eine PKCS7 Datei?

Eine PKCS7 Datei enthält die Digitalunterschrift und das Signatur-Zertifikat. Im Gegensatz zu s/Mime enthält es nicht die ursprünglichen Daten.

Was ist xmldsig?

Während eine XML-Datei unterzeichnet wird, ist es möglich, die Unterschrift direkt innerhalb des XML selbst abzulegen. Das wird xmldsig genannt.

Wie kann ich p7m und p7s Unterschriften gültig machen?

Klicken Sie mit der rechten Maustaste darauf und wählen "gültig machen"!

Index