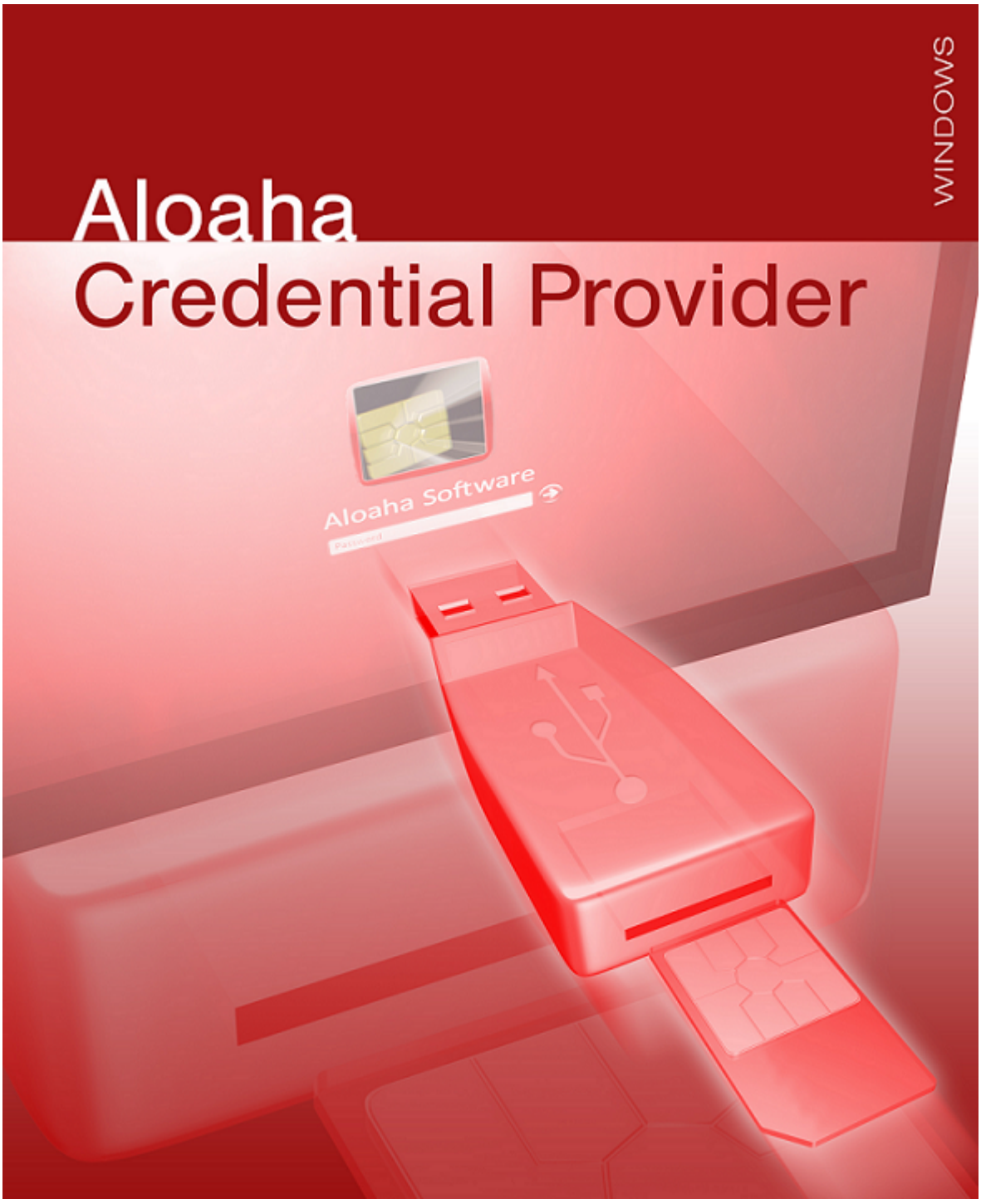


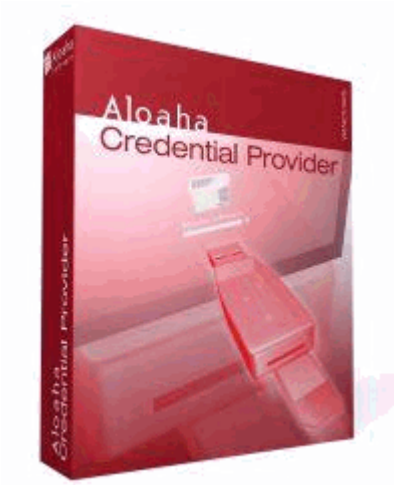
Aloaha Credential Provider DE

Aloaha Credential Provider DE

Druckdatum: Mai 2010

Inhalt

1. Einleitung



Aloaha jetzt mit eigenem Smartcard und Windows 7 Credential Provider

Eigenschaften der Aloaha Crypto Card:

- 3 unabhängige Schlüsselpaare + 1 verborgenes Schlüsselpaar
- Schlüssel können zur Karte hochgeladen oder auf der Karte selbst erzeugt werden
- 3 Zertifikat Container + 1 verborgenes Zertifikat
- Die PIN kann ausgeschaltet werden, um die Karte in einen einfachen Faktor 1 Authentifizierungsjeton umzuwandeln
- PUK, um die persönliche Geheimzahl zurückzusetzen
- Zusätzliches 32 Kilobyte (16 x 2 Kilobyte) zugesicherter Speicher. Zum Beispiel als Passwort-Safe für den Aloaha Credential Provider zu verwenden.

Beachten Sie, dass die Aloaha Crypto Card der ideale Behälter ist, um Ihre E-ID-Zertifikate aufzubewahren. Exportieren Sie das Zertifikat als PFX Datei und verschieben Sie es zur Karte.

Weiterhin wurde der Aloaha Credential Provider als Handbuch unter folgendem Link http://portal.aloaha.com/csp/Shared%20Documents/AloahaCredentialProvider.pdf veröffentlicht.

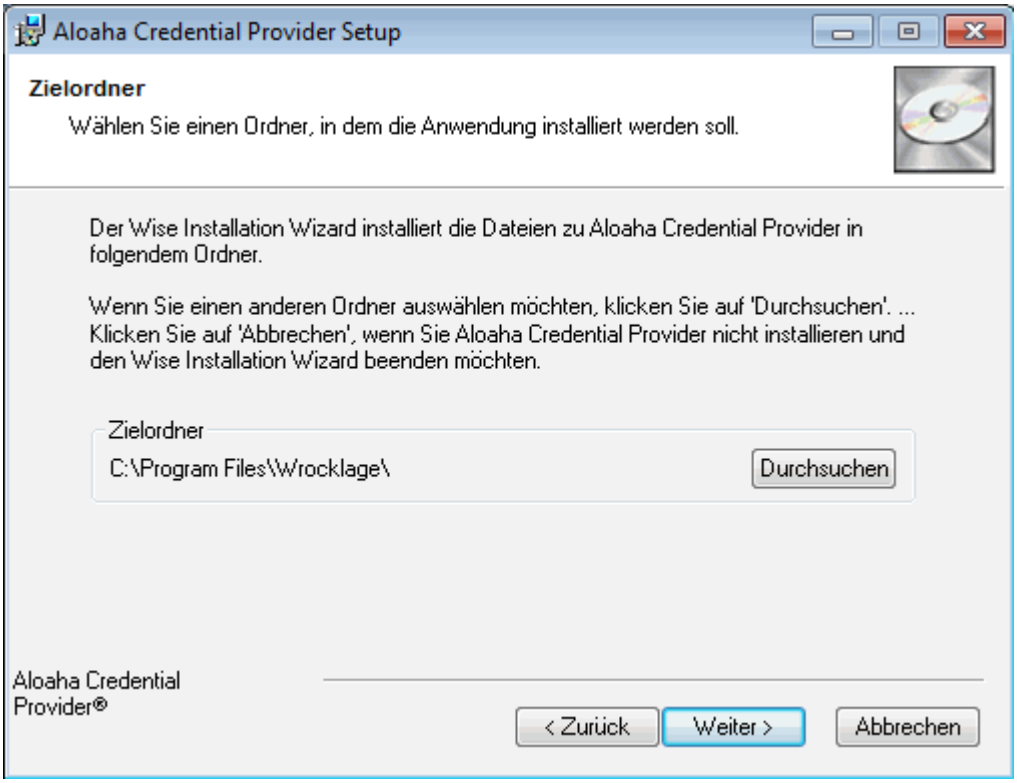
Systemvoraussetzungen

- Windows Vista/7, Windows 2008/Windows 2008R2
- Jede von Aloaha unterstützte Smartcard oder Aloaha Crypto Card

2. Installation

Den Aloaha Credential Provider können Sie sich direkt aus dem Internet unter http://www.aloaha.com/download/credentialprovider.zip herunterladen. Die Datei speichern Sie direkt auf Ihrer Festplatte. Sobald der Download beendet ist, entpacken Sie diese und doppelklicken auf "credentiaprovider.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.

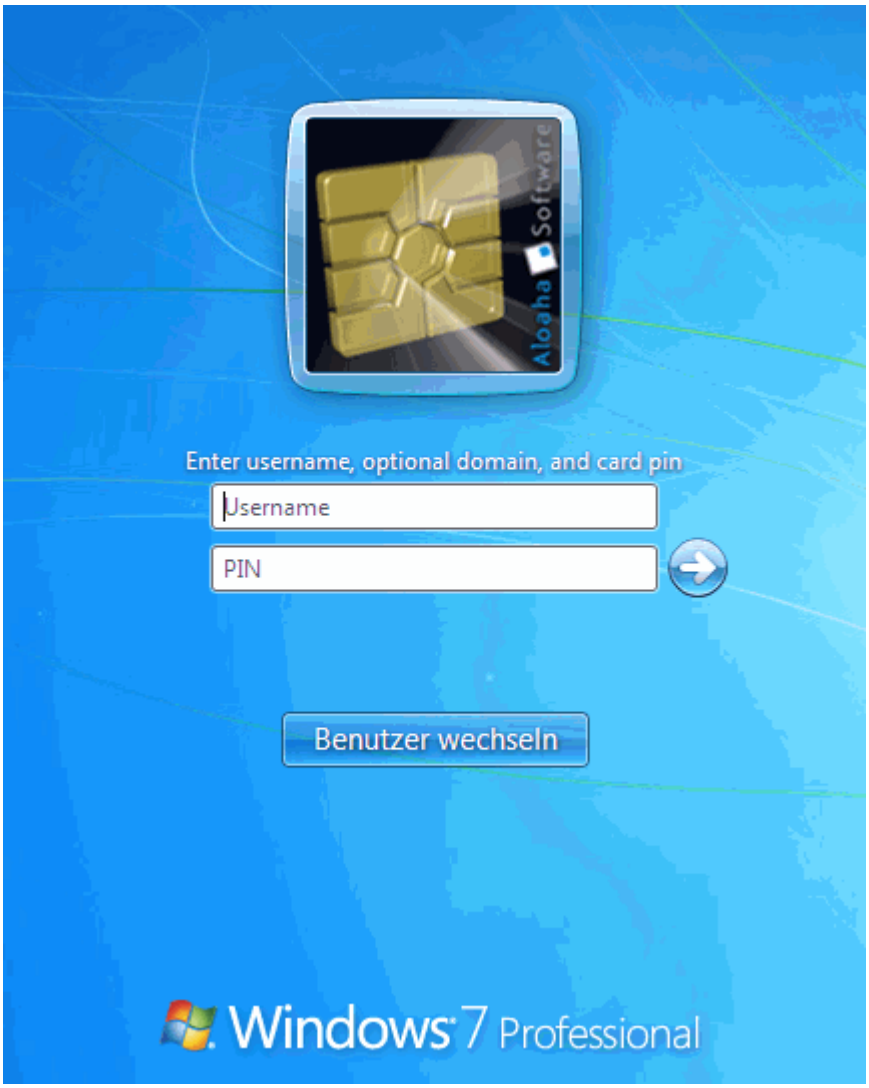


Nach der erfolgreichen Installation schließen Sie den Installationsvorgang mit "Fertigstellen" ab. Jetzt können Sie den Aloaha Credential Provider verwenden. In Ihrem Startmenü unter **Programme>Aloaha** finden Sie eine Verknüpfung zum Öffnen des Programmes.

3. Anwendung

Der neue Aloaha Credential Provider vertritt eine der dramatischsten Änderungen in Windows Vista / 7 Anmeldebildschirm, der es viel einfacher macht, neue Benutzerauthentifizierungen durchzuführen. Um die Anmeldung per Smartcard an eine Windowsmaschine zu ermöglichen, ist es i.d.R. nötig, dass der Anwender Mitglied einer Domäne ist. Mit dem Aloaha Credential Provider ist dies nicht mehr erforderlich!

Hier sehen Sie verschiedene Anmelde-Ikons. Das zweite Ikon zeigt den neuen Aloaha Credential Provider.



Die Funktion des Aloaha Credential Providers ist, das OS mit den Anmeldeinformationen zu versehen. Die Anmeldeinformationen werden verschlüsselt auf der lokalen Festplatte gespeichert. Sollte der Benutzer die Aloaha Crypto Card verwenden, ist der Ausweis zusätzlich auf der Karte verschlüsselt gespeichert. Wenn der Benutzer nun Benutzername, Domain\Username und PIN eingibt, entschlüsselt der Credential Provider die lokal gespeicherten Daten und gibt das System frei. Sie können die Felder auch leer lassen. In diesem Fall wird Aloaha die auf der Smartcard passendsten gefundenen Daten verwenden.

Um ein verschlüsseltes Passwort zu speichern, geben Sie "setpass:" gefolgt vom Passwort im 2. Feld ein.
Beispiel: `setpass:letmein`

Aloaha verschlüsselt das Passwort mit dem Zertifikat der Smartcard und speichert es lokal. Sollte die Aloaha Cryptocard verwendet werden, werden die Daten ebenfalls verschlüsselt und auf der Karte gespeichert.
Weiterhin gibt es einen Mechanismus, die verschlüsselten Daten über das Netzwerk zu synchronisieren.
Erstellen Sie einen Registrierungsschlüssel
`HKEY_LOCAL_MACHINE\SOFTWARE\Aloaha\CSP\RemoteUserPass` der auf eine Datei im Netzwerk oder eine URL verweist.
Der Inhalt könnte folgendermaßen aussehen: \\192.168.0.127\download\UserPass.ini oder http://192.168.0.127/download/UserPass.ini.
Solch ein Zugang würde bedeuten, dass wenn Aloaha lokal verschlüsselte Daten nicht findet, nach ihnen in der RemoteUserPass angegebenen Datei sucht.

Der Aloaha Credential Provider ist Bestandteil des Aloaha Cardconnector und kann von http://www.aloaha.com/download/cardconnector.zip heruntergeladen werden.

Um den Credential Provider zu aktivieren klicken Sie auf <Programm-Dateien>\wrocklage\z Register.reg

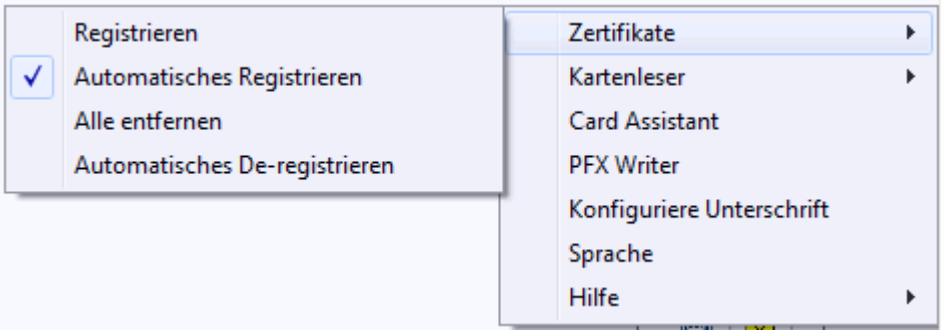
Ein oft verwendetes Scenario ist die Sekretär/-in Funktionalität. Ein Manager könnte die Karte seines/-r Sekretärs/-in in den Kartenleser einlegen, den setpass: Befehl eingeben und somit die Anmeldung des/-r Sekretärs/-in an seine Maschine OHNE den Inhalt seines Ausweises freizugeben, erlauben.

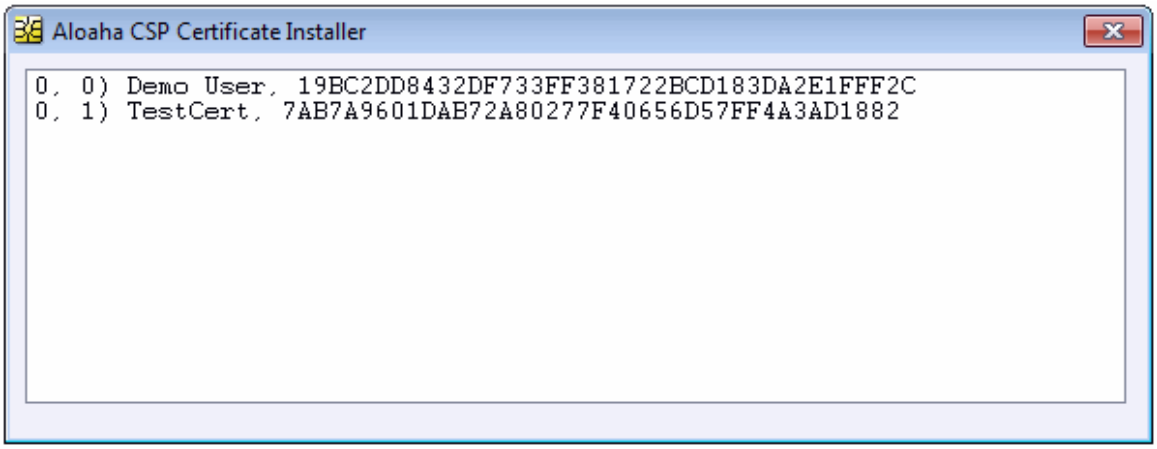
Der Aloaha Credential Provider beinhaltet einen von Microsoft anerkannten "Cryptographic Service Provider" (CSP) und eine PKCS #11 Bibliothek (aloaha_pkcs11.dll in system32).

Der Vorteil eines CSP besteht darin, dass der CSP die Zertifikate bereitstellt, die auf der Karte gespeichert sind.
Wenn der CSP ein Zertifikat des angemeldeten Users speichert, wird das Zertifikat in entsprechendem Verzeichnis abgelegt.

Um ein Video hierzu anzusehen, verwenden Sie nachfolgenden Link:
http://www.aloaha.com/movies/register.htm

Sobald eine Karte in ein Lesegerät gesteckt wurde, registriert das Programm automatisch alle auf der Karte befindlichen Zertifikate. Die Zertifikate können jedoch auch, wie im Beispiel gezeigt, manuell registriert werden. Statt Autoregister klicken Sie stattdessen auf Register.
Zum ersten Mal sollte ein Zertifikat manuell registriert werden, da dann Aloaha eventuell fehlende Root Zertifikate vom Aloaha Server nachlädt und mit installiert.





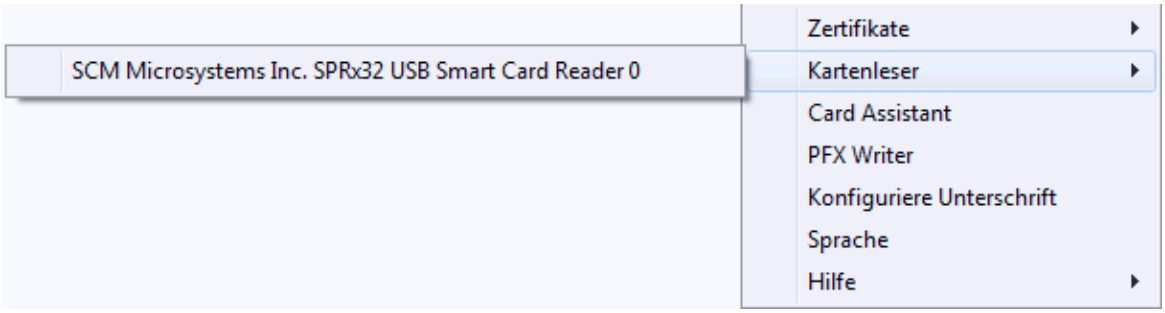
Die erste Zahl zeigt die Anzahl der Kartenlesegeräte an. Der Screenshot zeigt die Zertifikate der Karten in angeschlossenen Kartenlesern.
Die Zahl nach dem Komma zeigt den Zertifikat-Typ an.

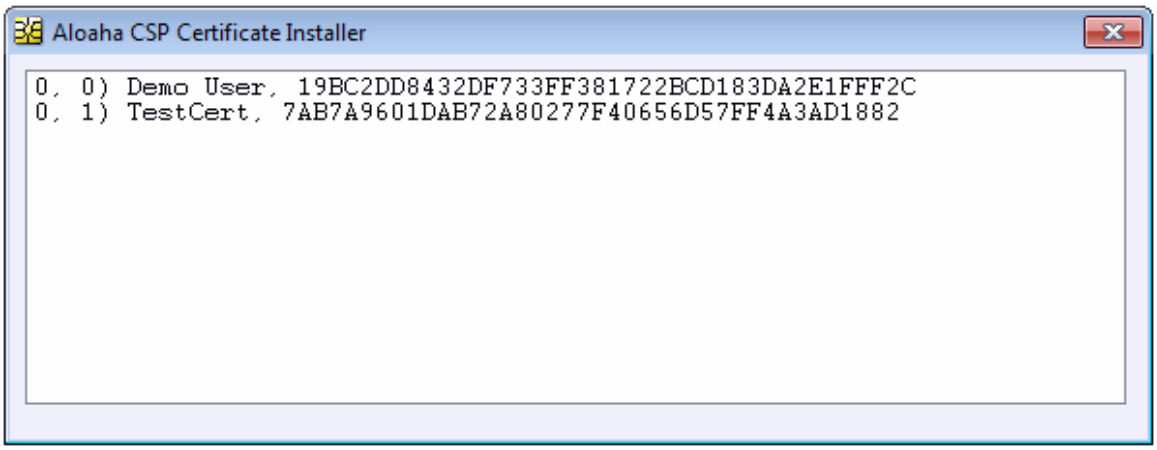
Typ 0 = Unterschriftszertifikat,
Typ 1 = Authentifizierungszertifikat,
Typ 2 = Verschlüsselungszertifikat.

Enthält eine Karte nur ein Zertifikat enthält, wird dieses als Typ 1 angezeigt.

Um alle registrierten Zertifikate zu entfernen, klicken Sie auf "alle entfernen". Ist Autoentfernen aktiviert, werden alle registrierten Zertifikate gelöscht, sobald sämtliche Karten aus den Kartenlesegeräten entfernt wurden.

In einigen Fällen gibt es mehrere mit einem System verbundene Kartenlesegeräte. Die Zertifikate aller Lesegeräte aufzuzählen, nimmt Zeit in Anspruch. In diesem Fall können Sie das Kartenlesegerät direkt (wie gezeigt) anwählen. Aloaha liest dann nur die Zertifikate der Karte im gewählten Leser aus.





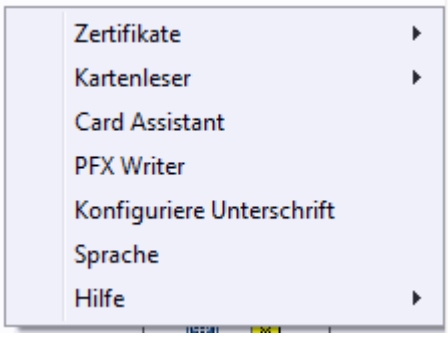
Sie können das Zertifikat nun anklicken, um es anzeigen zu lassen oder es per Doppelklick im aktuellen Verzeichnis zu speichern.

Manuelle Registrierung hat Vorteile:

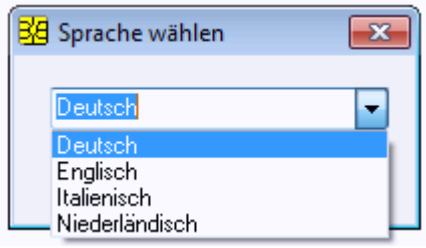
1. Wenn das Ausgabezertifikat im System nicht verfügbar ist, wird Aloaha versuchen, es von der Aloaha Website herunterzuladen.
2. Das eingetragene Zertifikat wird automatisch als Standardzertifikat konfiguriert.

3.1 Sprachauswahl

So ändern Sie die Anwendersprache unabhängig von der Systemsprache des Betriebssystems. Die Anwendersprache wird über das Traymenü geändert.

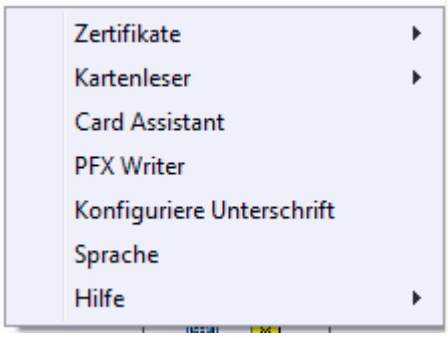


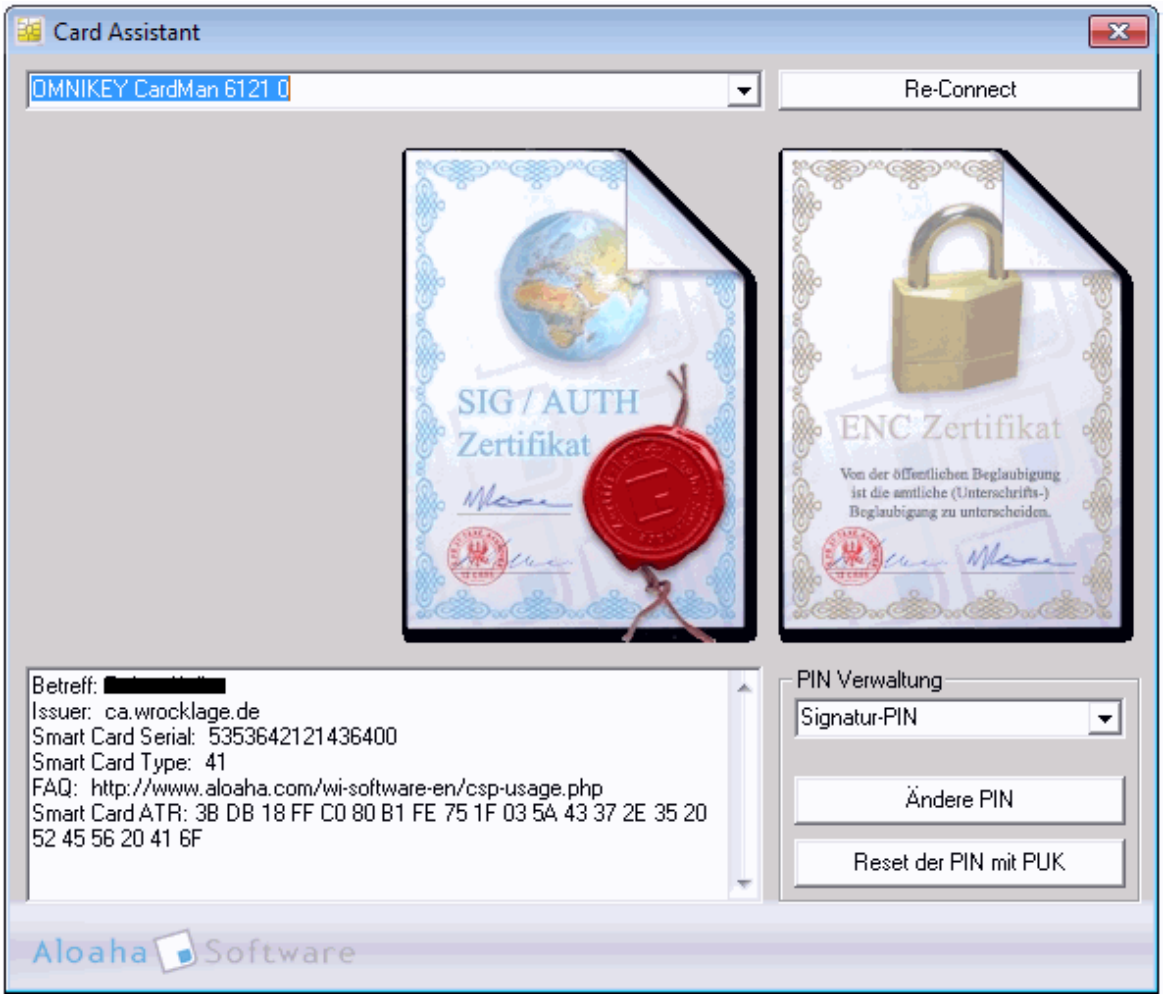
Zur Auswahl stehen die angezeigten Sprachen. Nachdem Sie die Sprache geändert haben, werden Sie aufgefordert, das Programm neu zu starten. Sollten Sie das Programm nicht neu starten, bleibt die bis dahin eingestellte Anwendersprache erhalten.



3.2 Kartenassistent

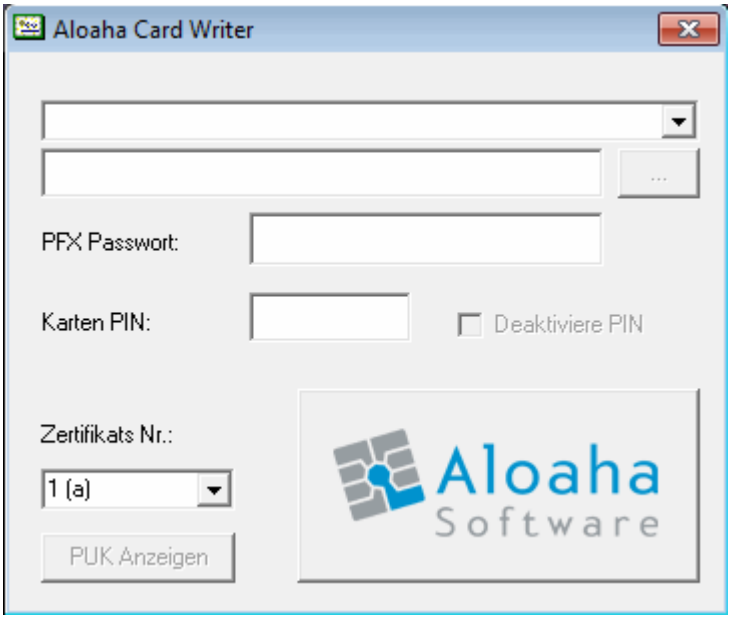
Der "Card Assistant" kann über das Windows Startmenü oder das Schnellstartmenü gestartet werden.





Durch das Auswahlmenü besteht die Möglichkeit alle im System verfügbaren Kartenleser auszuwählen. Je nach Karten-Typ können PINs oder PINs mit PUK geändert werden.

3.3 PFX Writer



Eine PFX-Datei enthält alle Informationen, aus denen ein digitales Zertifikat aufgebaut ist (PFX = Zertifikat + Public Key + Private Key), um zu signieren, authentifizieren oder entschluesseln. Solch eine PFX Datei kann mit dem Aloaha Card Writer direkt auf die Karte geschrieben werden.

PKCS steht für Public Key Cryptography Standards und bezeichnet eine Reihe von kryptografischen Spezifikationen.

Der Standard PKCS 12 definiert den Personal Information Exchange Syntax Standard. Dieser spezifiziert ein portierbares Dateiformat, welches dazu benutzt wird, private Schlüssel und zugehörige Public-Key-Zertifikate kennwortgeschützt zu speichern. PFX ist der Nachfolger von PKCS12. Dateien diesen Formats haben die Dateinamenerweiterung .PFX.

Als Zertifikatsnummern können

- 0 (s) - Container für Unterschriftszertifikate
- 1 (a) - Container für Authentifizierungszertifikate
- 2 (e) - Container für Verschlüsselungszertifikate

gewählt werden. Wenn man nur ein Zertifikat hat ist es ratsam, dieses in alle 3 Container zu schreiben.

Privaten Schlüssel und Zertifikat auf Karte schreiben

1. Wählen Sie den zu verwendenden Kartenleser. Anschließend geben Sie den Pfad zu der PFX - bzw. der Cer - Datei an.

2. Geben Sie das PFX Passwort ein, damit der Aloaha PFX Writer es entschlüsseln und auf die Karte schreiben kann. Das Passwort schützt die Datei vor unberechtigtem Zugriff. Wenn das Kennwort nicht eingegeben wird und das PFX verschlüsselt ist kann das PFX nicht auf die Karte geschrieben werden.

3. Geben Sie die Karten PIN ein. Diese wird benötigt, um die PIN zu aktivieren oder zu deaktivieren. Zum schreiben des PFX ist die PIN nicht nötig!

4. Klicken Sie auf den Aloaha Button und schreiben damit den privaten Schlüssel und das entsprechende Zertifikat auf die Karte.

3.4 Digital Signieren

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 Weg Daten unterzeichnet werden können.
Denn das Hauptproblem bei der Übermittlung elektronischer Daten ist die leichte Manipulierbarkeit. Erst durch die elektronische Signatur kann dieses Problem behoben werden, da eine unbemerkte Datenmanipulation nicht mehr möglich ist.

Voraussetzung hierfür ist, dass die elektronische Signatur wie eine handschriftliche 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, der Zertifikatsinhaber also 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 geschlossen 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 in den Computer übertragen.

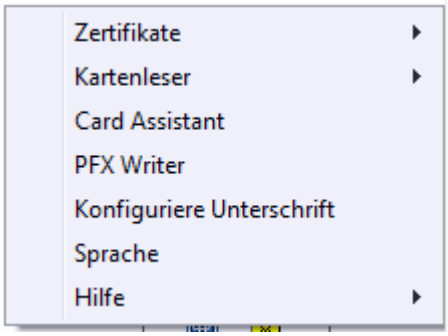
Um den privaten Schlüssel zu benutzen, wird die richtige PIN benötigt, die zusätzliche Sicherheit gewährleistet. Die Signatur kann also nur vom Karteninhaber sein, denn nur er ist in Besitz von Karte und PIN. Der öffentliche Schlüssel ist in ein Zertifikat integriert und steht jedermann in Verzeichnisdiensten im Internet zur Verfügung oder kann per E-Mail versand werden. Um zu gewährleisten, dass dieses Zertifikat und somit der Schlüssel nicht gefälscht wurde, lässt sich die Signatur des Herausgebers prüfen.

Beim Prüfen der Signatur wird der öffentliche Schlüssel des Empfängers verwendet, so dass nur dieser die Daten mit seinem privaten Schlüssel wieder entschlüsseln kann. 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. Die verschlüsselten Daten werden anschließend wieder in den Computer zurückgeschickt. Vorher muss der private Schlüssel durch die richtige PIN (Personal Identification Number) freigegeben werden.

3.4.1 Konfiguration digitale Unterschrift

CSP Symbol Menüleiste (rechte Maustaste)

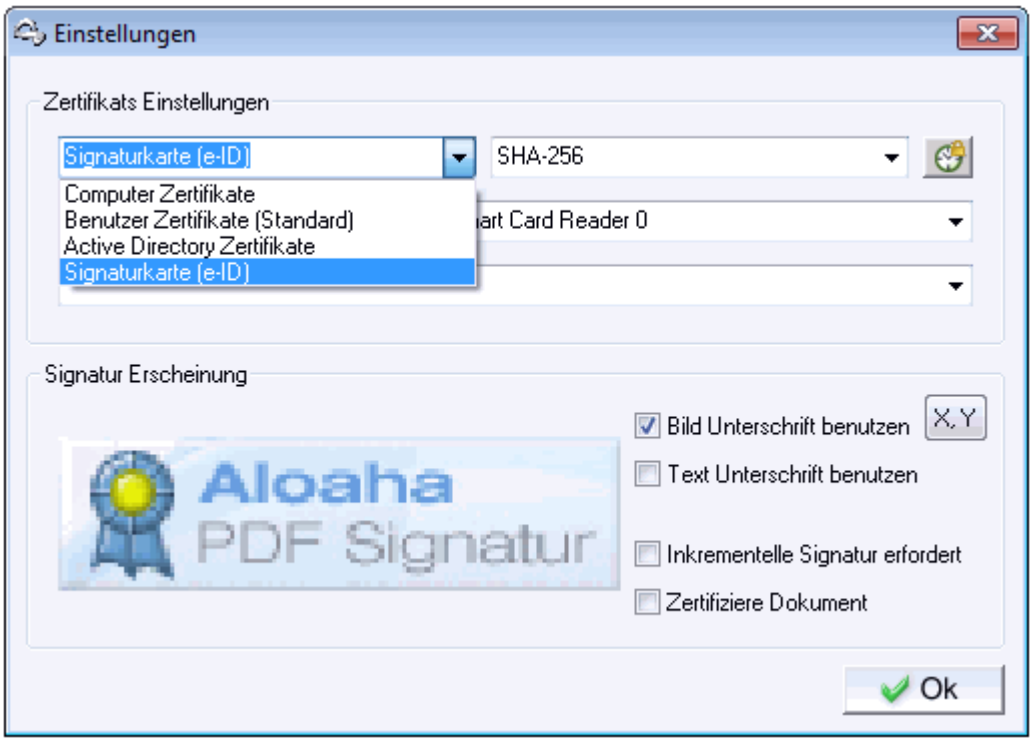


1. Zertifikatquelle

Hier können Sie zwischen verschiedenen Arten von Zertifikaten wählen, die Sie zum Signieren Ihrer PDF-Dateien verwenden möchten.

Zur Auswahl stehen:

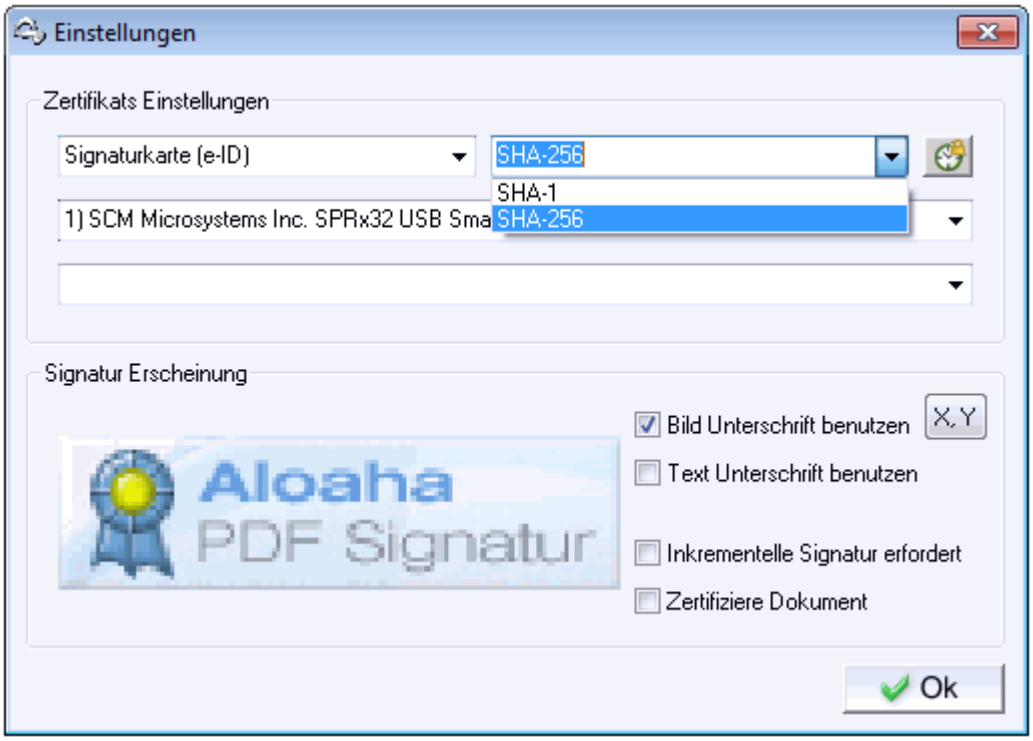
- **Computer Zertifikate**
  Es werden in der Zertifikats-Auswahlliste alle Zertifikate angezeigt, die dem Computer zugeordnet sind.
- **Benutzer Zertifikate (Standard)**
  Es werden in der Zertifikats-Auswahlliste alle Zertifikate angezeigt, die dem aktuellen Benutzer zugeordnet sind.
- **Active Directory Zertifikate**
  Es werden in der Zertifikats-Auswahlliste alle Zertifikate angezeigt, die im Active Directory zur Verfügung stehen.
- **SmartCard (e-ID)**
  Es werden in der Zertifikats-Auswahlliste alle angeschlossenen Kartenleser angezeigt.



2. Art des Zertifikats

Hier können Sie die Zertifikatsliste der angezeigten Zertifikate nach besonderen Zertifikat-Attributen filtern.

Wenn als Zertifikatsquelle "Smartcard" ausgewählt wird, können Sie zwischen SHA-1 und SHA-256 als Signatur-Algorithmus auswählen. SHA-256 ist sicherer und länger gültig, jedoch können nicht alle Chipkarten diesen Algorithmus bedienen.



3. Zertifikat auswählen

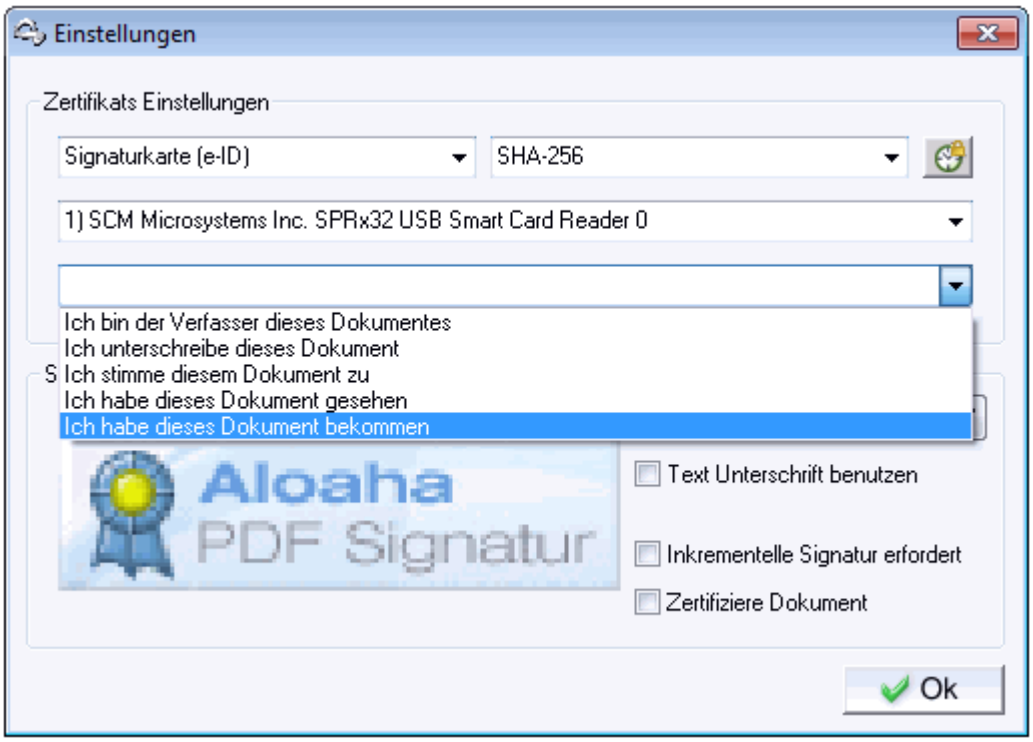
Dieses Menü hängt von der Zertifikatquelle ab. Wählen Sie "Benutzerzertifikat", erhalten Sie in diesem Feld eine Auflistung aller Benutzerzertifikate auf Ihrem PC und können das entsprechende Zertifikat auswählen.
Wählen Sie als Zertifikat die SmartCard (e-ID), erscheint eine Auflistung aller zur Zeit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

4. Zweck der Signatur

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

Man kann auch frei einen Text eingeben



Text Unterschrift

Ist die Option "Text Unterschrift benutzen" gewählt, wird der in dem 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. Im Signaturvorgang wird dieser Platzhalter durch das aktuelle Datum und der Name des Zertifikatinhabers ersetzt.

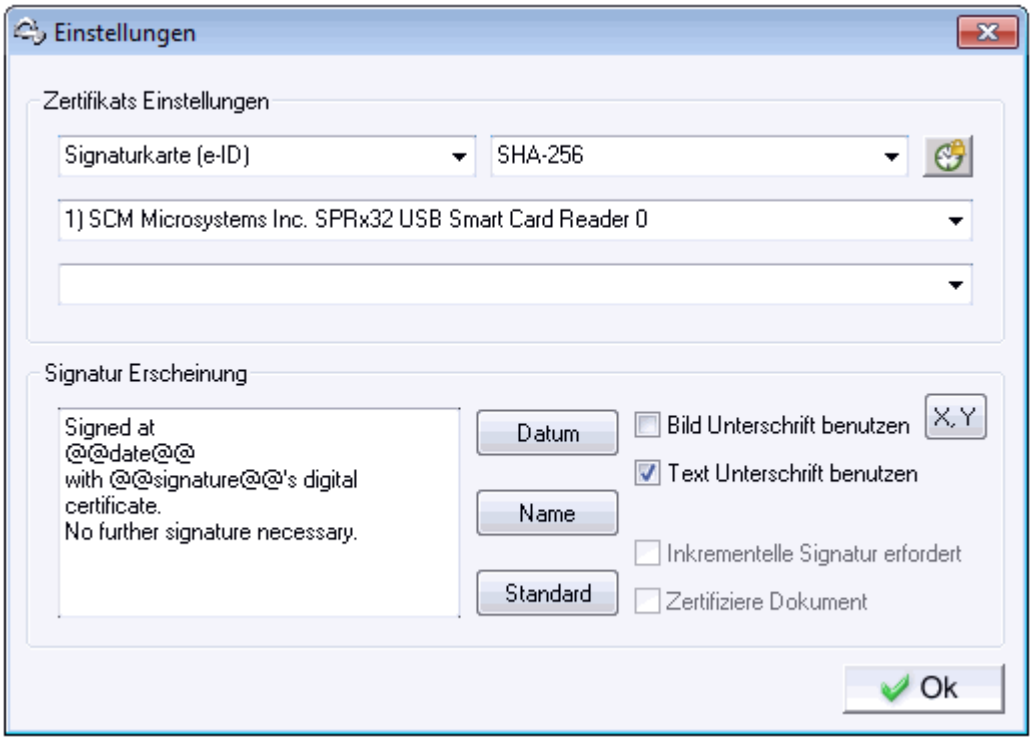
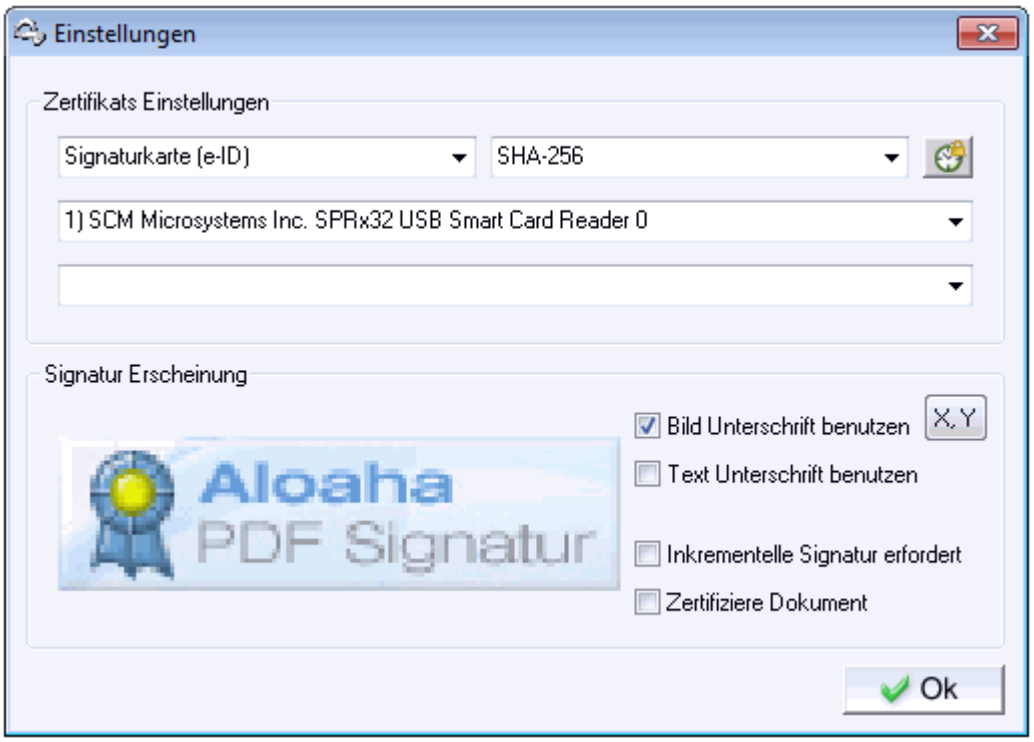


Bild Unterschrift

Sie haben natürlich auch die Möglichkeit, das Dokument durch eine Bildunterschrift zu signieren. Näheres zu den Einstellungen finden Sie unter "Signatureinstellungen"



5. Einstellungen für den Zeitstempel

Wenn Sie auf das Uhren-Symbol neben der Auswahl für die Art des Zertikates klicken öffnet sich ein weiteres Fenster.
Näheres zu den Einstellungen des Zeitstempels finden Sie unter "Zeitstempel"

6. Position der Signatur

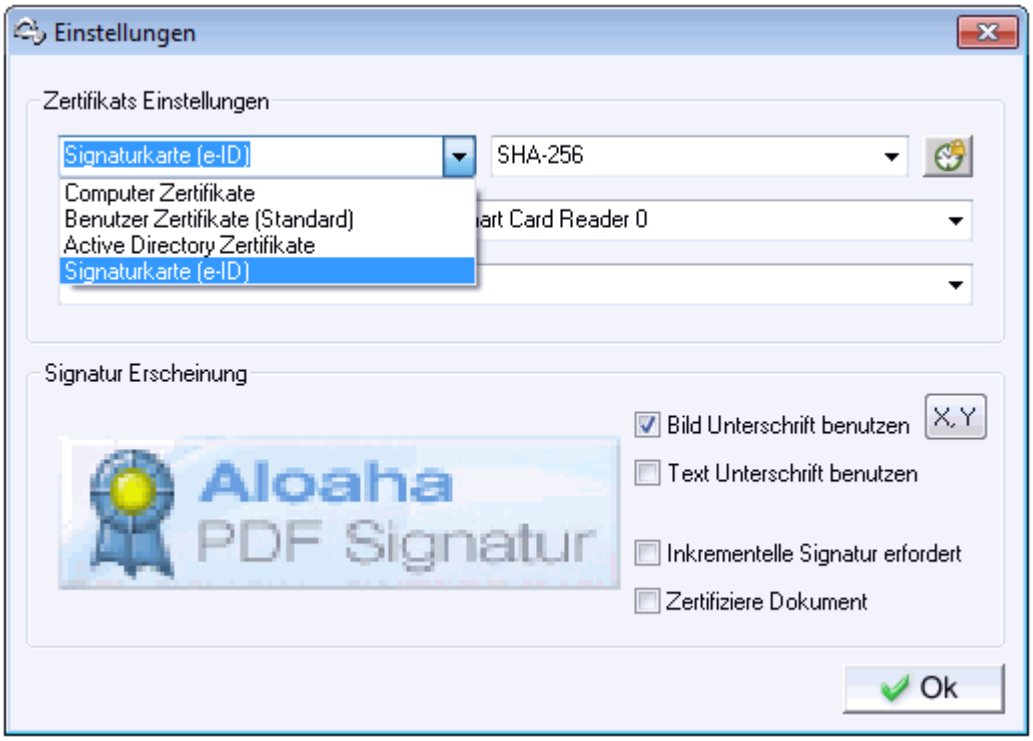
In den vier Feldern geben Sie die Position der Signatur vor. Hierbei wird immer in % der Seitengr öße gerechnet. Das Koordinatensystem startet mit 0% links unten auf dem PDF. Unter "oben links" konfigurieren Sie die linke obere Ecke des Signaturfeldes, angefangen in der X-Achse. Unter "unten rechts" 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. Nun fahren Sie mit der Maus die gewünschte obere linke Ecke der gewünschten Position an und klicken einmal mit der linken Maustaste. Danach fahren Sie die rechte untere gewünschte Position an und klicken noch einmal mit der linken Maustaste. So haben Sie die Position dann festgelegt.

3.4.2 Signatureinstellungen

Wenn Sie in der Menüleiste mit der rechten Maustaste auf das Symbol klicken, gelangen Sie zu den Signatur-Einstellungen

In den Zertifikats-Einstellungen kann die Art des Zertifikates gewählt werden, mit der ein Dokument signiert werden soll.
Das zu signierende Dokument kann im Explorer mit Klick auf die rechte Maustaste gewählt werden.
Für den Fall, dass Sie ein PDF Dokument signieren möchten, ist es möglich, zwischen unterschiedlichen Signaturen zu wählen.



Anstatt eines sich im System befindlichen Zertifikates kann ggf. auch ein Kartenlesegerät als Signatur-Datenquelle gewählt werden.

Dies kann bei Verwendung mehrerer Signatur-Karten hilfreich sein. Das Karten-Lesegerät ist in den Grundeinstellungen als Datenquelle bereits definiert.
In diesem Fall nutzt Aloaha die Signatur der Karte des konfigurierten Lesegerätes.
Der Vorteil besteht darin, dass der Anwender die Unterschriftseinstellungen bei Nutzung weiterer Karten nicht erneut konfigurieren muss.

Um die Sigantur zu ändern, klicken Sie auf die Grafik. Anschließend können Sie das Bild austauschen.

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!

Mit diesem Programm ist es möglich, die Signatur mit einem Zeitstempel zu versehen. Um den Zeitstempel zu konfigurieren, klicken Sie auf das Uhrensymbol.
Der https://tsa.aloaha.com ist ein unabhängiger Zeitstempel-Server, der von Aloaha bereitgestellt wird.
Falls Sie http://AloahaTimestamper gewählt haben, verwendet das Programm die lokale Systemzeit, um die Signatur mit einem Zeitstempel zu versehen.

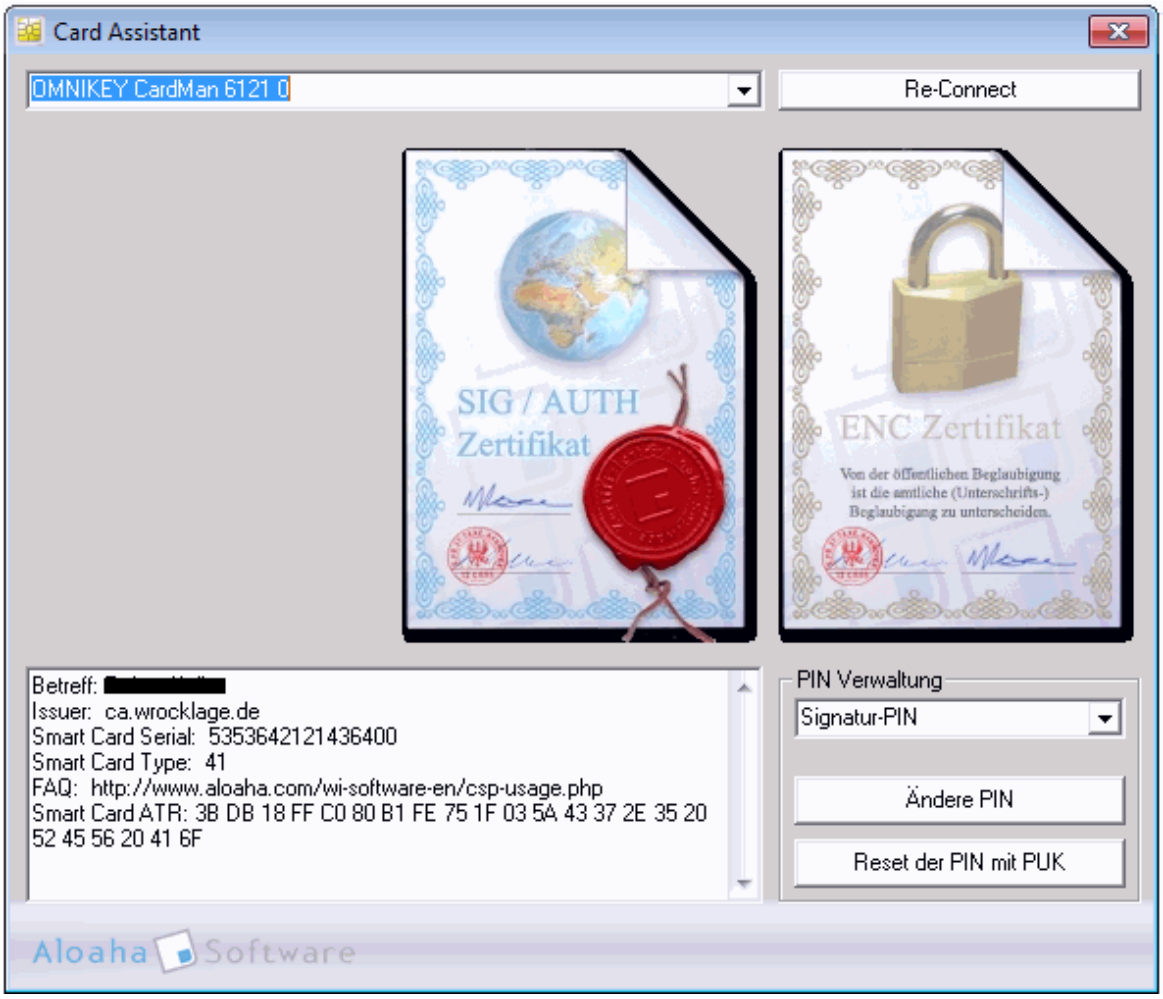
Hinweis: Viele Zeitstempel-Berechtigungen sind nicht RFC 3161 kompatibel, daher erteilt Aloaha dem Anwender keine Befugnis, weitere Berechtigungen zu vergeben.
Für weitere Berechtigungen, wenden Sie sich schriftlich an aloaha@wrocklage.de

3.5 PIN Verwaltung

Über das Auswahlmenü **Aloaha Card Assistant** können Sie folgende PIN´s verwalten:

Signatur-PIN
Karten-PIN
PIN Home

Hier können PIN´s geändert oder zurückgesetzt werden.



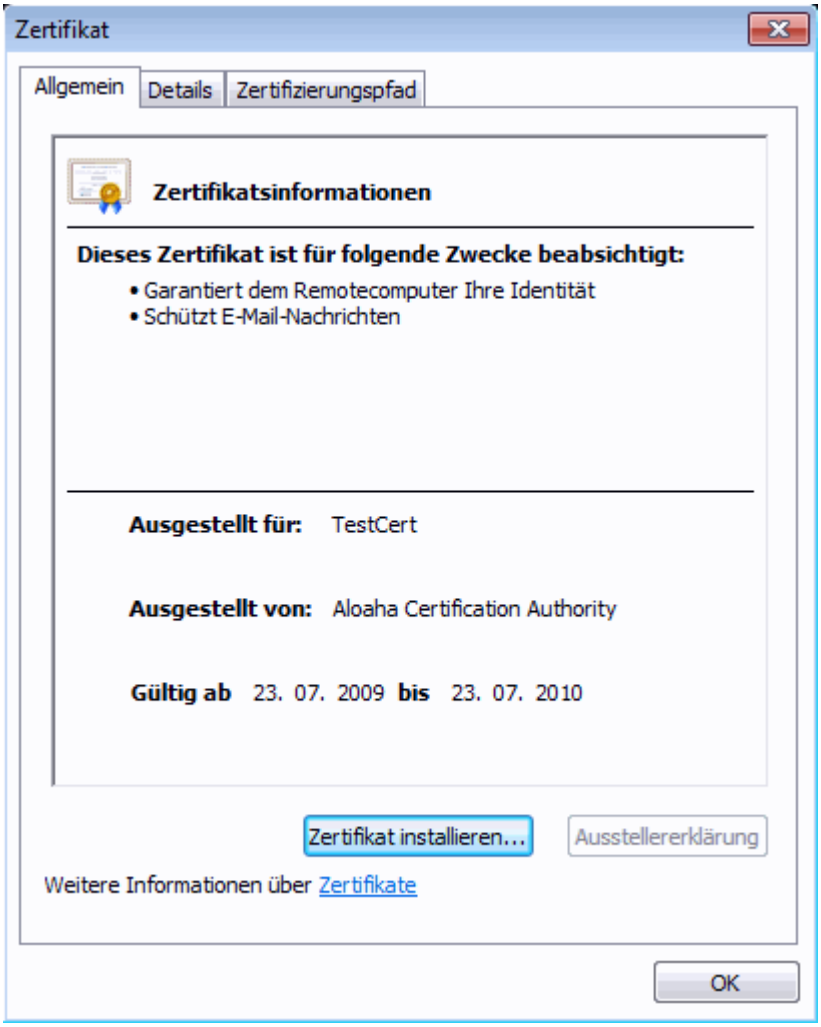
Nachdem Sie mit der Maus auf den Button **Ändere PIN** geklickt haben, erscheint foldendes Bild

Geben Sie zunächst die "**Alte PIN**" über die PC-Tastatur ein, anschließend die "**Neue PIN**" und bestätigen Sie die Eingabe mit "OK". Danach ist der Vorgang abgeschlossen und die entsprechende PIN geändert.

3.6 Zertifikate

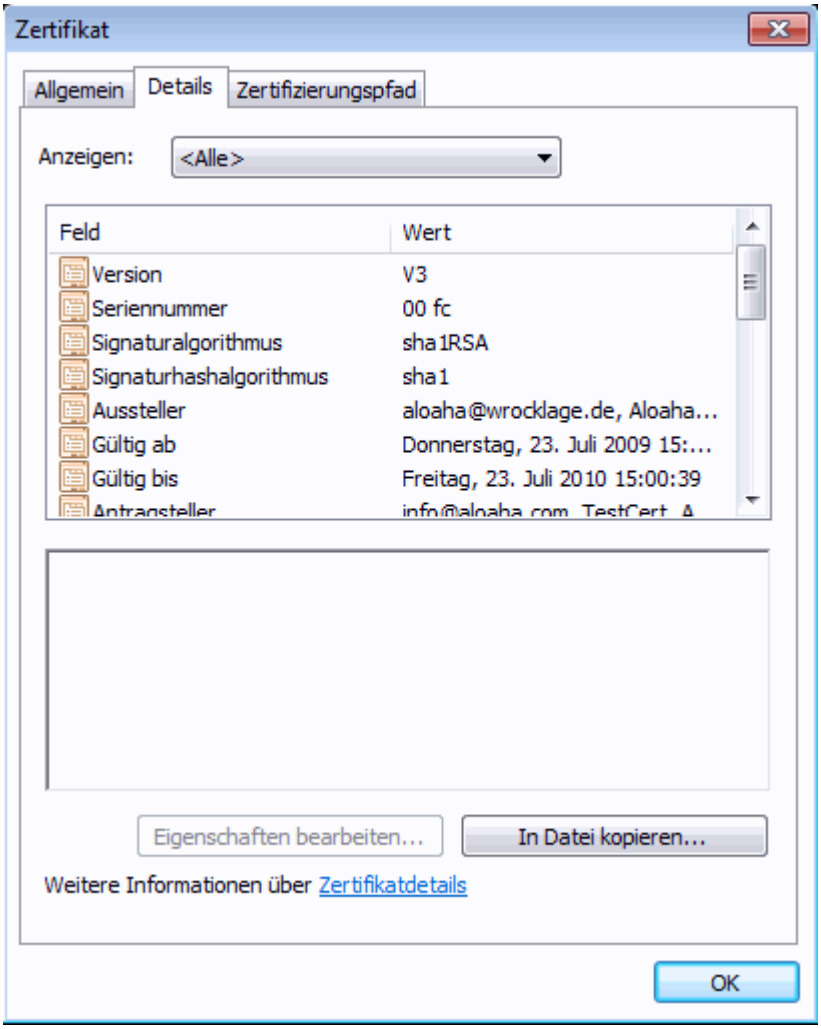
Allgemeine Zertifikatsinformationen

Um Inforamtionen zu den Zertifikaten zu erhalten, rufen Sie den Card Assistant auf. Klicken Sie auf eines der im Card Assistant enthaltenen Zertifikate und Sie erhalten im Reiter "**Allgemein**" die Informationen zum ausgewählten Zertifikat. Hier wird angezeigt, wie lange das Zertifikat noch gültig ist, ob es ggf. abgelaufen ist, wer das Zertifikat ausgestellt hat und welchen Namen das Zertifikat trägt.



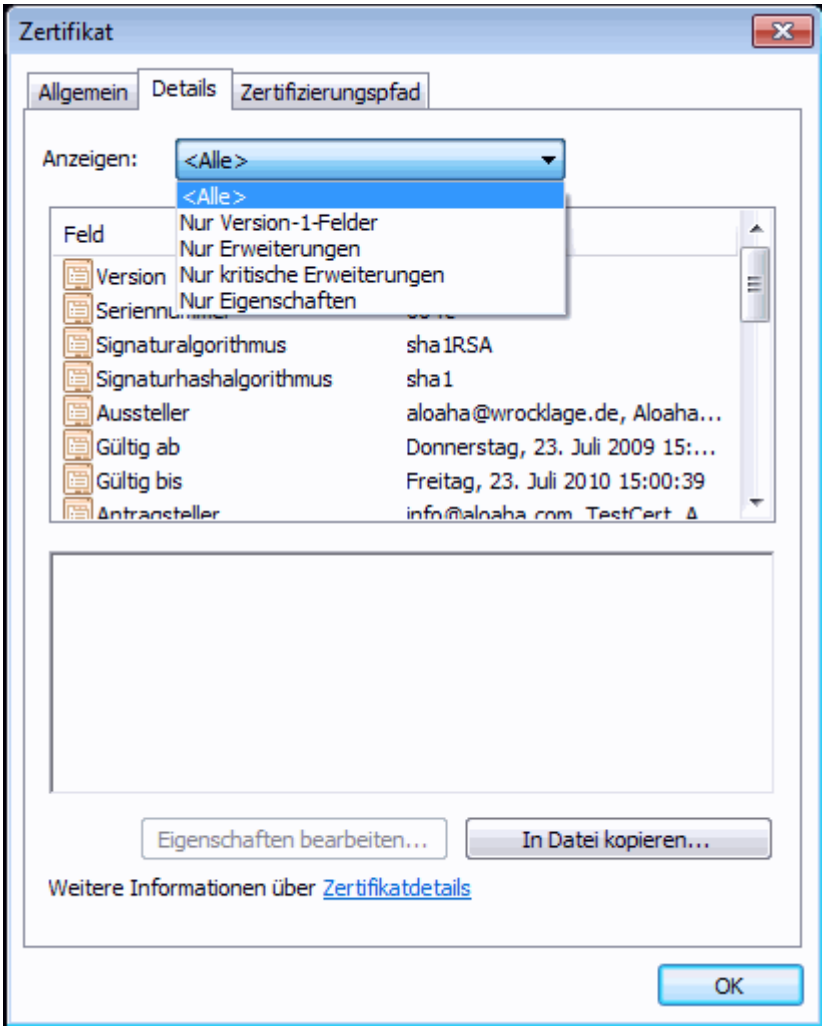
Im Reiter "Details" finden Sie weitere Informationen zum jeweiligen Zertifikat, wie z.B.:

- Version
- Seriennummer
- Signaturalgorithmus
- Aussteller
- gültig ab
- gültg bis
- Antragsteller
- öffentlicher Schlüssel
- ...
-



Sie können sich durch das Auswahlmenü folgende Informationen zum jeweiligen Zertifikat anzeigen lassen:

- Alle
- Nur Version-1-Felder
- Nur Erweiterungen
- Nur kritische Erweiterungen
- Nur Eigenschaften

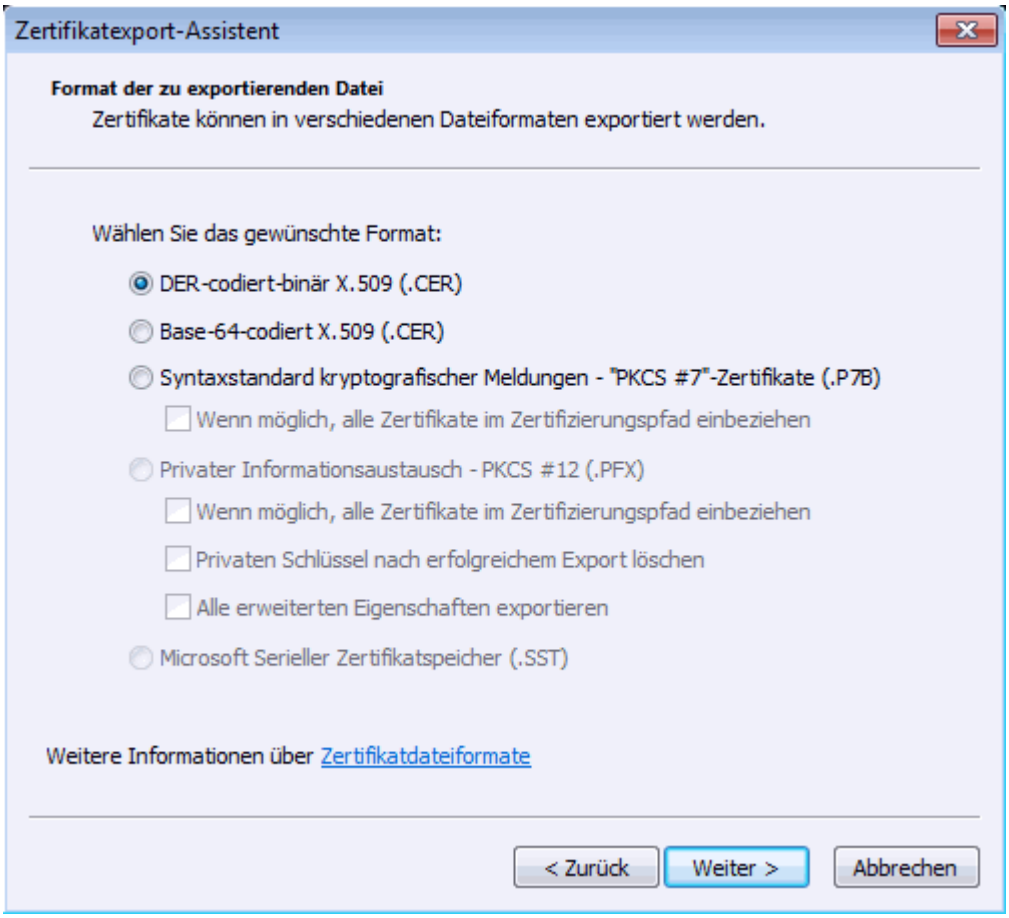


Zum Zertifikatsexport-Assistent gelangen Sie, wenn Sie in vorher gezeigtem Bild "In Datei kopieren" wählen.

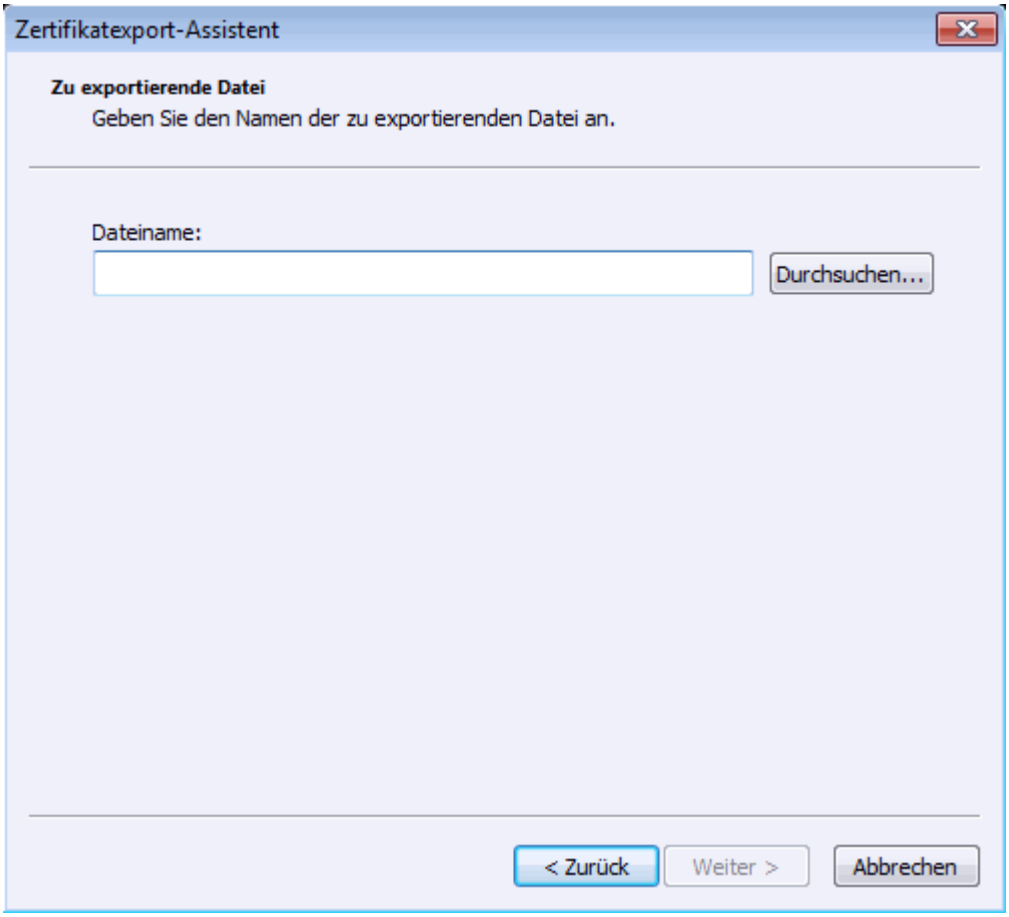
Nachdem Sie mit "Weiter" bestätigt haben, öffnet sich ein Fenster, wobei Sie das Exportdateiformat auswählen können.

Mögliche Exportformate:

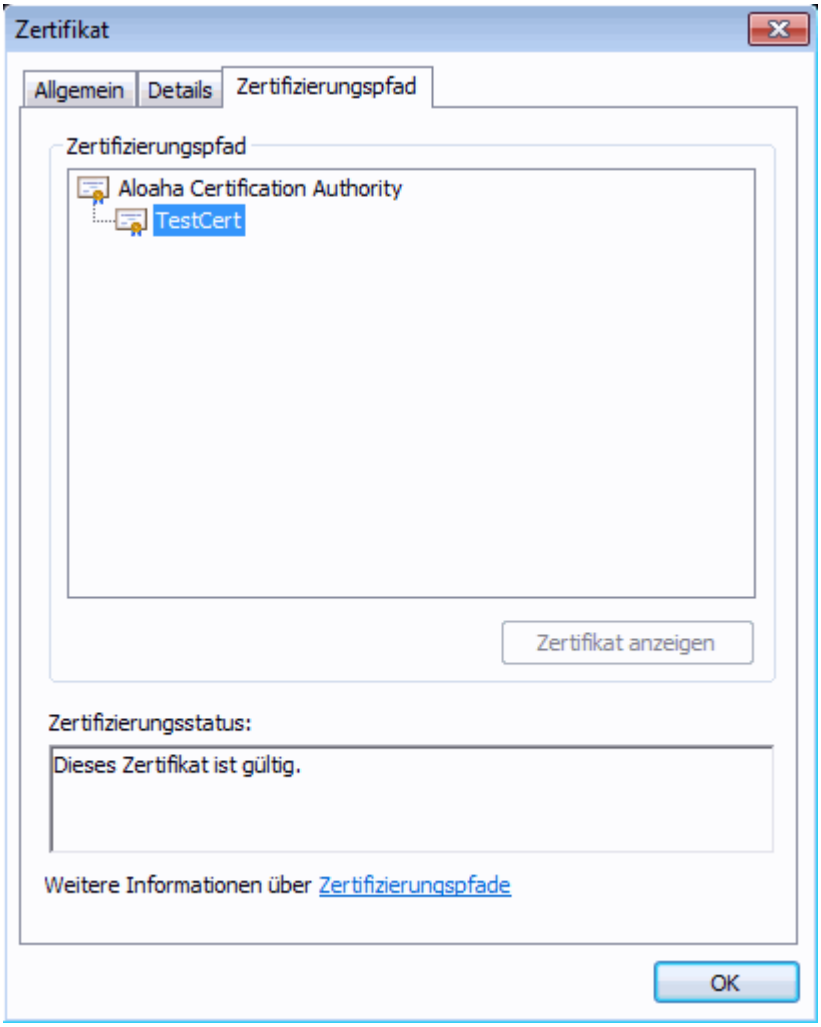
DER-codiert-binär X.509 (.CER)
Base-64-codiert X.509 (.CER)
Syntxstandard kryptografischer Meldungen - PKCS #7-Zertifikate (.P7B)



Nachdem Sie das Dateiformat ausgewählt haben, bestätigen Sie mit "Weiter" und gelangen zur Eingabe der zu exportierenden Datei.

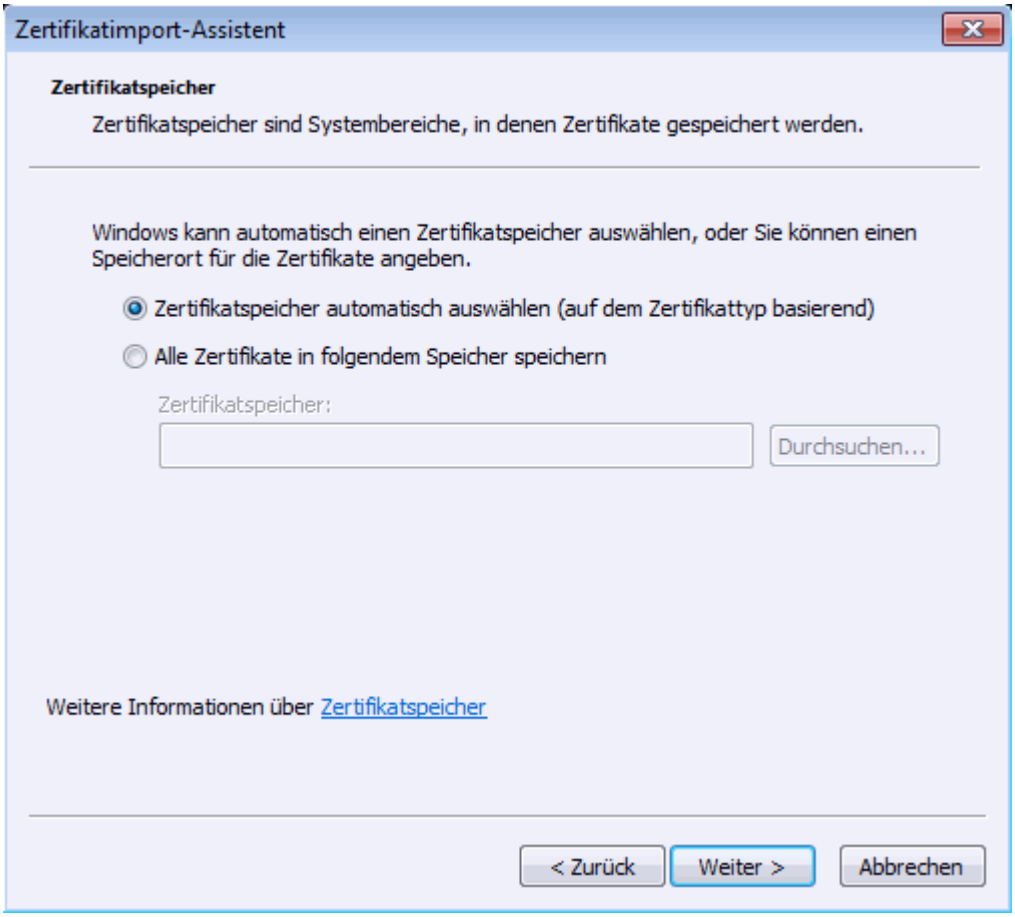


Der Zertifizierungspfad gibt an, wer Ersteller ist und um welche Art des Zertifikates es sich handelt.

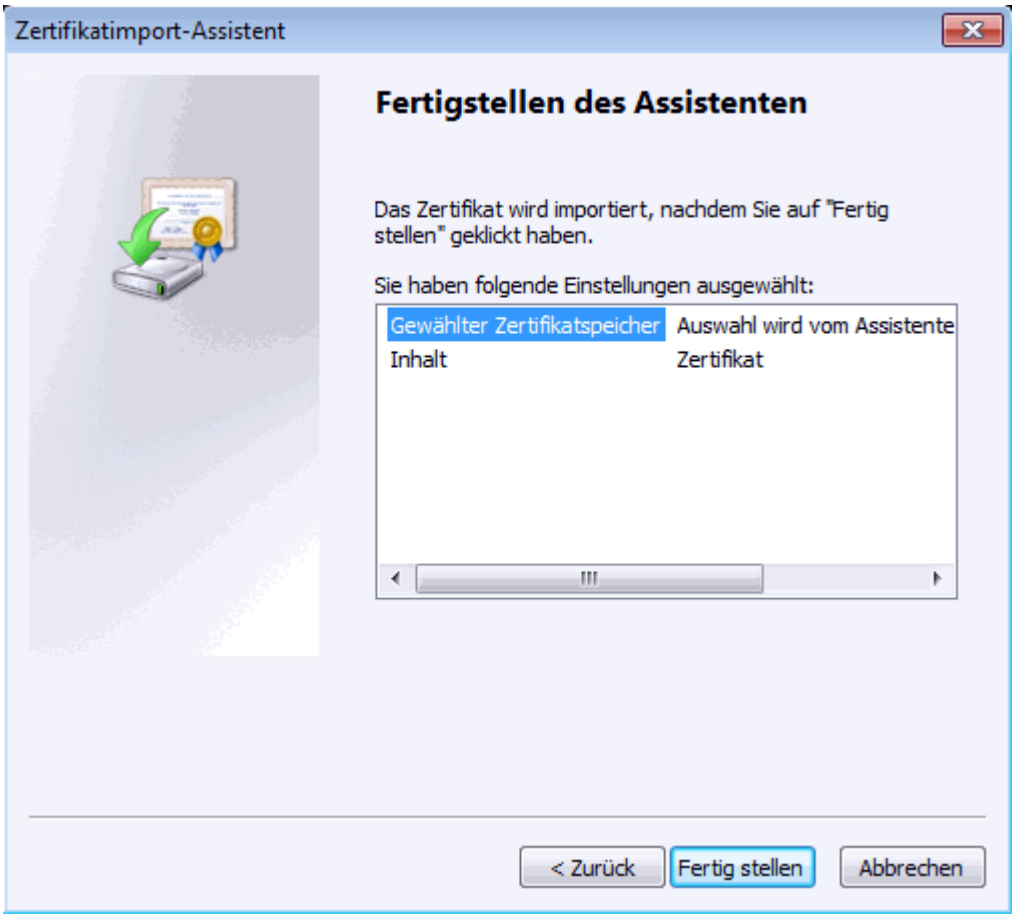


Zum Zertifikatsimport-Assistent gelangen Sie, indem Sie im Reiter "Allgemein" auf Zertifikat installieren klicken. Anschließend öffnet sich folgendes Fenster. Mit "Weiter" setzen Sie den Vorgang fort.

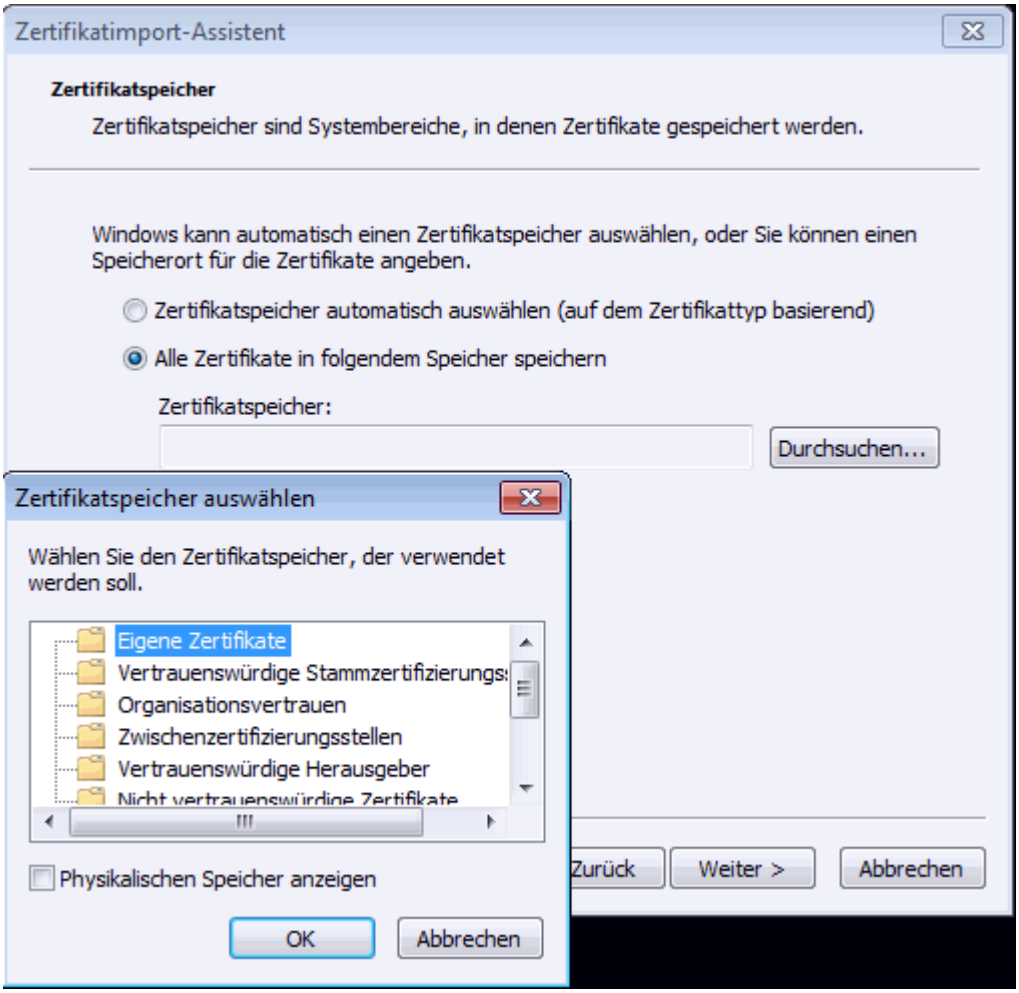
Hier wählen Sie den Zertifikatspeicher entweder basierend auf dem Zertifikattyp automatisch aus oder legen fest, an welchem von Ihnen vorgegebenen Speicherort Zertifikate gespeichert werden.



Nachdem Sie die Auswahl mit Weiter bestätigt haben, erhalten Sie im folgenden Informationen über die gewählten Einstellungen. Mit "Fertigstellen" wird der Vorgang abgeschlossen.



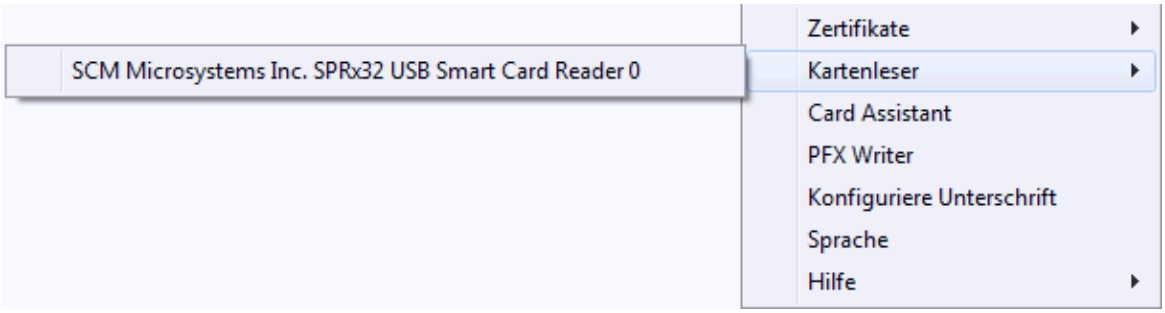
Sie haben nicht nur die Möglichkeit, Zertifikate automatisch durch den Assistenten zu speichern. Falls Sie sich dazu entscheiden, den Zertifikatspeicher selbst auszuwählen, aktivieren Sie das entsprechende Feld und wählen den Speicherort selbst aus der dann erscheinenden Liste aus. Anschließend bestätigen Sie die Auswahl mit OK.



3.7 CSP / Kartenleser

Unterstützte Kartenleser

Aloaha unterstützt derzeit ca. 45 Kartenleser der Sicherheitsklasse 2 und 3. Sie wurden nach dem deutschen Signaturgesetz bestätigt und dürfen zur Erzeugung qualifizierter elektronischer Signaturen eingesetzt werden.



Sobald eine Karte in ein Lesegerät gesteckt wurde, registriert das Programm automatisch alle auf der Karte befindlichen Zertifikate. Die Zertifikate können jedoch auch manuell registriert werden. Statt Autoregister klicken Sie stattdessen auf Register.

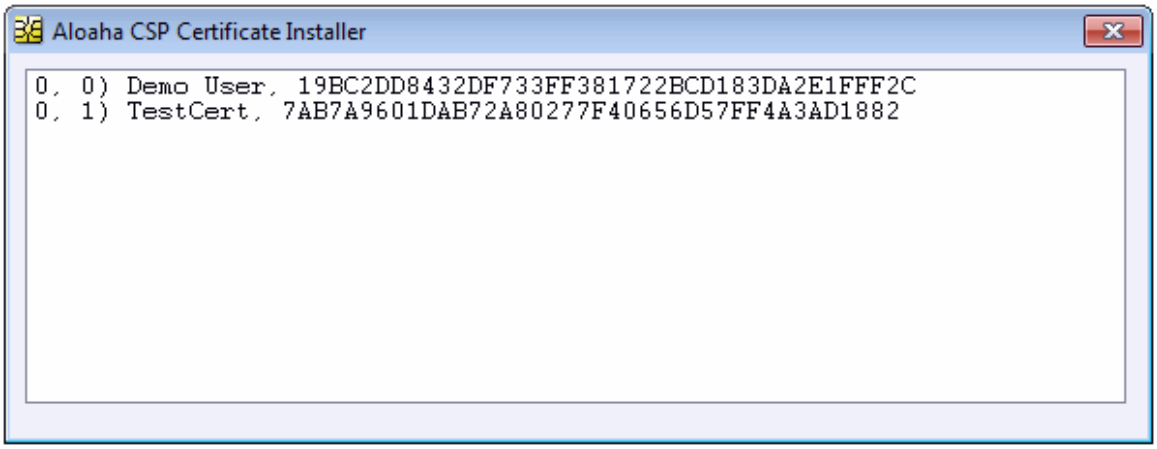
Die erste Zahl zeigt die Anzahl der Kartenlesegeräte an. Der nachfolgende Screenshot zeigt die Zertifikate der Karte(n) in angeschlossenen Kartenlesern.
Die Zahl nach dem Komma zeigt den Zertifikat-Typ an.

Typ 0 = Unterschriftszertifikat,
Typ 1 = Authentifizierungszertifikat,
Typ 2 = Verschlüsselungszertifikat.

Enthält eine Karte nur ein Zertifikat enthält, wird dieses als Typ 1 angezeigt.

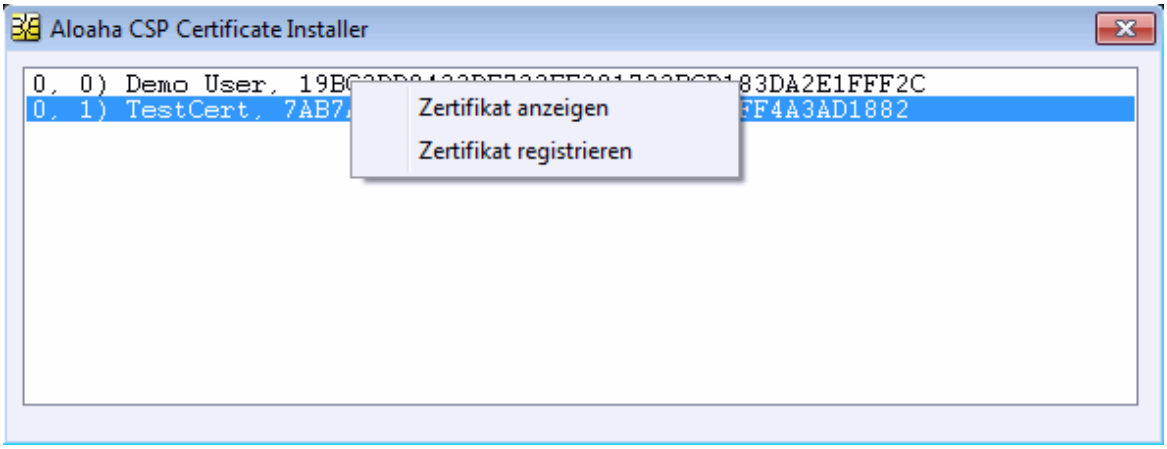
Um alle registrierten Zertifikate zu entfernen, klicken Sie auf "alle entfernen". Ist Autoentfernen aktiviert, werden alle registrierten Zertifikate gelöscht, sobald sämtliche Karten aus den Kartenlesegeräten entfernt wurden.

Kartenleser



In einigen Fällen gibt es mehrere mit einem System verbundene Kartenlesegeräte. Die Zertifikate aller Lesegeräte aufzuzählen, nimmt Zeit in Anspruch. In diesem Fall können Sie das Kartenlesegerät direkt anwählen. Aloaha liest dann nur die Zertifikate der Karte im gewählten Leser aus.

Sie können das Zertifikat nun anklicken, um es anzeigen zu lassen oder es per Doppelklick im aktuellen Verzeichnis zu registrieren.



Manuelle Registrierung hat Vorteile:

1. Wenn das Ausgabezertifikat im System nicht verfügbar ist, wird Aloaha versuchen, es von der Aloaha Website herunterzuladen.
2. Das eingetragene Zertifikat wird automatisch als Standardzertifikat konfiguriert.

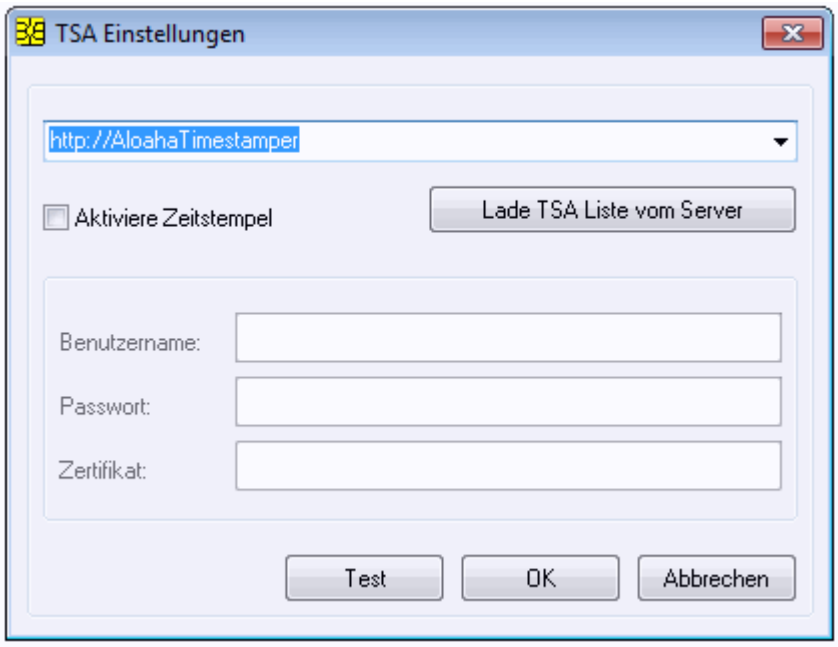
Sicherheitswarnung bei Zertifikat anzeigen / registrieren

Wenn Sie ein Zertifikat registrieren, erhalten Sie eine Sicherheitswarnung. Lesen Sie sich den Inhalt durch
und entscheiden anschließend, ob Sie das Zertifikat registrieren / installieren möchten oder nicht.
Der Dialog erscheint NUR wenn **ERSTMALIG** ein neues Root Zertifikat eingepflegt wird!

3.8 Zeitstempel

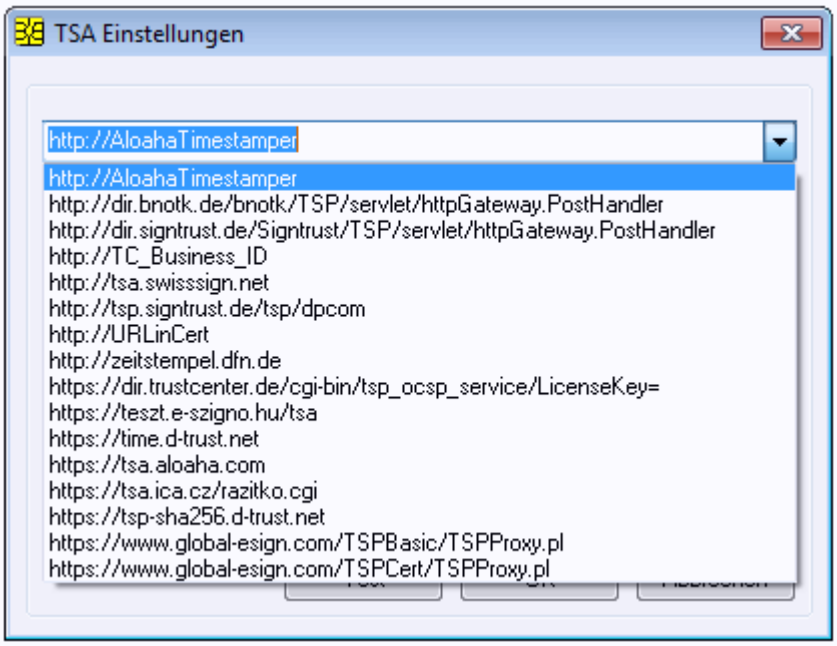
Einstellungen für den Zeitstempel

Wenn Sie auf das Uhren-Symbol im Signatur-Konfigurationsmenü klicken öffnet sich nachfolgend gezeigtes Fenster für die Zeitstempeleinstellungen:



Hier können Sie die Einstellungen für den integrierten RFC 3161 kompatiblen Zeitstempel Client anpassen.
Im oberen Feld wählen Sie einen verfügbaren Zeitstempelserver aus. Ist die Liste leer, können Sie die Liste der möglichen Zeitstempelserver durch Klick auf den Button "Lade TSA Liste von Server" von der Aloaha Webseite herunterladen.

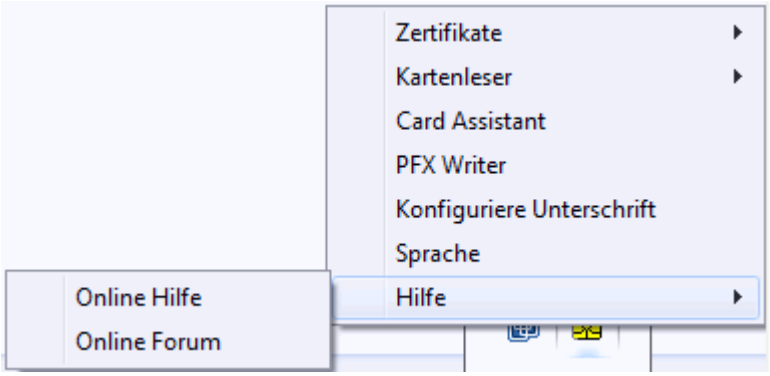
Wenn Sie http://AloahaTimestamper auswählen, wird der TimeStamp-Server benutzt. Hierbei wird die Lokale Systemzeit als Grundlage für den Zeitstempel genommen.
Unter Benutzerdaten konfigurieren Sie Ihre Zugangsdaten zum jeweiligen Zeitstempeldienst.



4. Hilfe

So gelangen Sie zur Online Hilfe und dem Online Forum im Internet: http://www.aloaha.de/support/aloaha-credentialprovider.php

Die Online Hilfe bzw. das Online Forum kann über das Windows Startmenü oder das Schnellstartmenü gestartet werden. Wählen Sie anschließend den entsprechend benötigten Menüpunkt.



5. FAQ

Ist es möglich, den Standardanmeldelogon zu entfernen, wenn der Credential Provider verwendet wird?
Ja. Erstellen sie folgenden Registrierungsschlüssel

[HKEY_USERS\.DEFAULT\Software\Aloaha\CP]
"CredentialProviderFilter"="1"

oder doppelklicken Sie auf die Datei "Set Aloaha Key to activate Filter" im Aloaha Installationsordner.

Kann ich die lizenzfreie Software Aloaha Crypt verwenden, wenn ich eine Lizenz für den Credential Provider besitze?
natürlich

Gibt es einen Passwort-Safe für den Internet Explorer?
Mailen sie uns (info@aloaha.com), um den Download-Link zu erhalten.

Werden 64-Bit-Betriebssysteme unterstützt?
Ja

Index