Benutzerhandbuch

AutoSigner

Version 1.0.32

MENTANA-CLAIMSOFT GMBH
Ein Unternehmen der FP-Gruppe

Berlin/Fürstenwalde
Trebuser Str. 47
Haus 1
15517 Fürstenwalde

Bad Salzdetfurth/Niedersachsen
Griesbergstr. 8
D-31162 Bad Salzdetfurth

Mentana-Claimsoft GmbH
Griesbergstraße 8
D-31162 Bad Salzdetfurth
Germany

Tel: +49 5063 / 2 77 44 -0
Fax: +49 5063 / 2 77 44-50

Service Center Signaturprodukte: 01806/ Signatur (74462887)

(0,20 € pro Anruf aus dem deutschen Festnetz, max. 0,60 € pro Anruf aus dem deutschen Mobilfunknetz)

E-Mail: info@mentana.de
Internet: www.mentana-claimsoft.de

Inhaltsverzeichnis

1 DOKUMENTENVERLAUF

Version	Datum	Änderung	Verfasser
1.0.0	18.08.04	Erstellung	MS
1.0.1	26.08.04	Überarbeitung	AJA, MS
1.0.2	12.01.05	Anpassung der Oberfläche	MS
1.0.4	11.04.05	INI-Datei Anpassung	MS
1.0.6	14.09.05	Diverse Anpassungen der GUI	JL
1.0.20	13.09.06	Anpassungen an die aktuelle Version	SW
1.0.28	26.02.09	Bilder aktualisiert	SB
1.0.29	15.04.10	Hinweise BNetzA	RK
1.0.30	06.10.15	Bilder aktualisiert, Smartcard-Modul	DP
1.0.31	07.12.16	Anpassungen an die neue Version	DP
1.0.32	17.07.17	Anpassungen CI	OM

2 VORBEMERKUNG

Bei dem Produkt AutoSigner' handelt es sich um ein Produkt, das nach § 3 SigG der Aufsicht durch die Bundesnetzagentur unterliegt.

Die zuständige Aufsichtsbehörde für qualifizierte Signaturen und unterstützende Produkte ist die Bundesnetzagentur (ehemals Regulierungsbehörde für Telekommunikation und Post (Reg TP)) als Bundesoberbehörde im Geschäftsbereich des Bundesministeriums für Wirtschaft und Technologie mit Sitz in Bonn, Tulpenfeld 4, 53113 Bonn, Telefon: 02 28/14-0, www.bundesnetzagentur.de.

Bitte lesen **vor Inbetriebnahme die Herstellererklärung gemäß § 17 Abs. 4 SigG** zu diesem Produkt wie Sie bei der Bundesnetzagentur veröffentlicht wurde.

In der Herstellererklärung erhalten Sie alle verbindlichen Informationen über:

- zulässige Einsatzumgebung
- potezielle Bedrohungen
- zulässge Komponenten und Systeme
- Auflagen des Herstellers

3 EINFÜHRUNG

Mit dem ‚AutoSigner' können elektronische (digitale) Signaturen für eine beliebige Anzahl von Dokumenten erstellt und in das Ursprungsdokument integriert werden. Der ‚AutoSigner' ist als eigenständige Applikation, die keine Adobe-Produkte voraussetzt und auf einer Workstation oder einem Server einsetzbar ist.

Eine grafische Übersicht hierzu zeigt: Abbildung 1

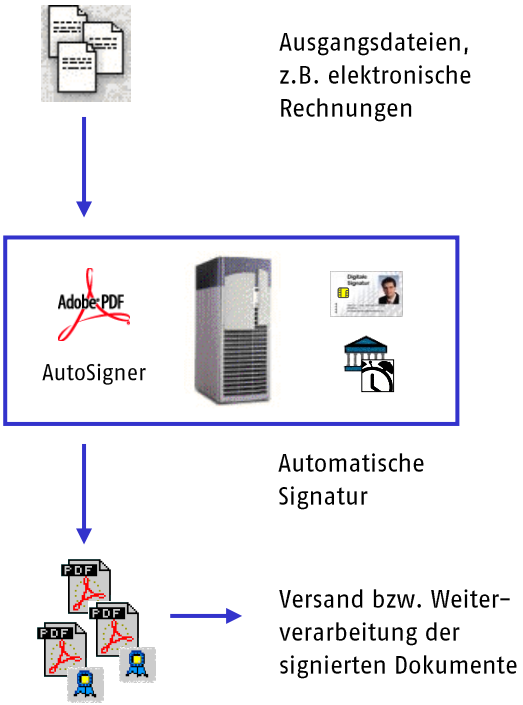

Abbildung 1 – AutoSigner Übersicht

Zu den wichtigsten Funktionen des AutoSigner zählen:

- Automatisches Einfügen von digitalen Unterschriften, sichtbar und unsichtbar, in einer größeren Anzahl von Dokumenten
- Signieren beliebig vieler Dokumente, dabei wird eine externe Signatur (.pkcs7) erzeugt.
- Auswahl eines Zertifikates, aus den auf dem Rechner bzw. auf angeschlossenen Signaturkarten verfügbaren Zertifikaten

Hinweis:

Die Unterschriften von bereits unterschriebenen PDF Dokumenten können mit dem 'PDF Signer', ein Plug-In für Adobe® Acrobat® ab Version 5.0 oder Adobe® Reader ab Version 5.1, oder dem ‚AutoVerifier', einer Portallösung (http://www.signaturportal.de) zur Verifikation überprüft werden.

4 SYSTEMVORAUSSETZUNGEN

Für die Installation der Software gelten folgende Systemvoraussetzungen:

- Betriebssysteme/ Kartenlesegeräte/ SmardCards: **siehe Herstellererklärung**
- Zum Signieren: Ein auf den Signierer ausgestelltes, gültiges Zertifikat als Softwarezertifikat oder auf einer SmartCard
- Installierter kryptografischer Serviceprovider (CSP) [Bestandteil des Produktes]

Bei dem kryptografischen Serviceprovider (CSP) handelt es sich um eine Software, die in Form einer DLL auf dem Rechner installiert sein muss. Dieser CSP hat die Funktion, mit einer SmardCard zu kommunizieren und sämtliche kryptografischen Anforderungen durchzuführen. Der CSP sowie eine entsprechende Installationsroutine wird dem Anwender in der Regel vom Zertifikatsherausgeber zur Verfügung gestellt.

Abbildung 2 – Hardwarekomponenten für den AutoSigner

5 INSTALLATION

5.1 CD-ROM

1. Legen Sie die ‚AutoSigner' Produkt CD in Ihr CD-ROM Laufwerk.
2. Starten Sie anschließend das Installationsprogramm „Setup.exe" im Stammverzeichnis der Produkt CD (*Laufwerk*:\). Verwenden Sie hierzu den Windows Explorer oder die Windows Kommandozeile.
3. Es erscheint ein Begrüßungsdialog. Folgen Sie den Anweisungen des Installationsassistenten.
4. Nach Abschluss der Installation kann sofort mit dem ‚AutoSigner' gearbeitet werden.

5.2 DOWNLOAD

1. Starten Sie die heruntergeladene Autosigner-xxx.msi
2. Es erscheint ein Begrüßungsdialog. Folgen Sie den Anweisungen des Installationsassistenten.
3. Nach Abschluss der Installation kann sofort mit dem ‚AutoSigner' gearbeitet werden.

6 BEDIENUNG

6.1 PRINZIPIELLE ARBEITSWEISE

Nach dem ersten Start des ‚AutoSigners' sollten vor dem ersten Signaturvorgang einige Einstellungen vorgenommen werden.

Je nach Auswahl der Einstellungen signiert der ‚AutoSigner' Dokumente, zu festgelegten Zeitpunkten, nach Ablauf eines definierten Zeitintervalls, oder eine festgelegte Anzahl, automatisch.

6.2 ALLGEMEINE EINSTELLUNGSMÖGLICHKEITEN

Über den Menüpunkt ‚Einstellungen' stehen die Optionen: Allgemein, Signatur, Sprache, Module und Smartcard-Unterstützung zur Verfügung.

Wird unter dem Menüpunkt ‚Einstellungen' der Unterpunkt ‚Allgemein' ausgewählt, öffnet sich ein, Registerkartenfenster für allgemeine Einstellungen.

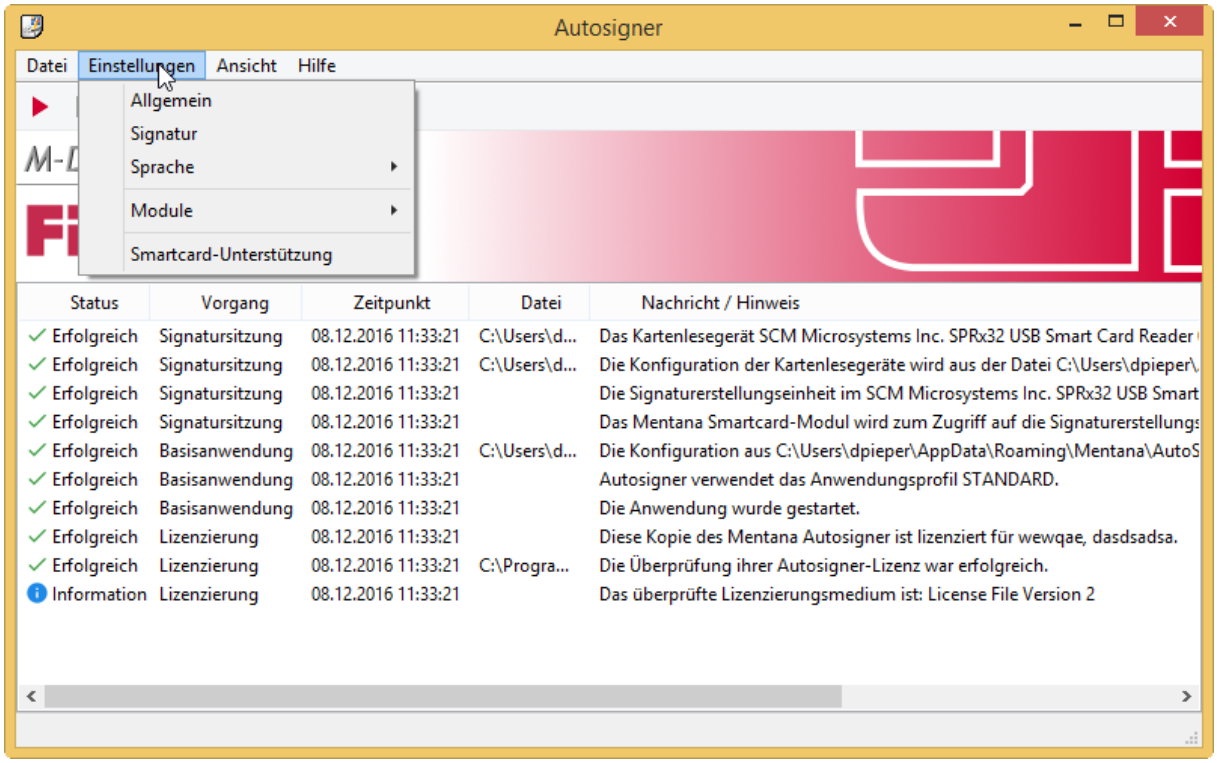

Abbildung 3 – Einstellungen

6.2.1 BETRIEBSMODUS

Unter "Allgemein -> Allgemein" kann entschieden werden, welche Schnittstelle für das Signieren von Dokumenten verwendet werden soll. Als Standard-Einstellung ist die Dateibasierte Schnittstelle festgelegt. Hierbei werden die Vorgänge von der Anwendung selbst überwacht, die Dateien signiert und in das konfigurierte Verzeichnis kopiert.

Für weitere Schnittstellen benötigt man separate Lizenzen, welche bei der Mentana-Claimsoft AG käuflich erworben werden können. Zu diesen zählt, eine ‚SOAP-Schnittstelle', wodurch die Anwendung über eine Webserviceschnittstelle gesteuert werden kann und eine ‚SMTP-Schnittstelle', welche die Anwendung als transparenten Proxy-Server innerhalb einer E-Mail-Infrastruktur laufen lässt. Als AutosignerPro-Knoten, welcher die Anwendung als einen Knoten innerhalb der Autosigner-Pro-Installation konfiguriert.

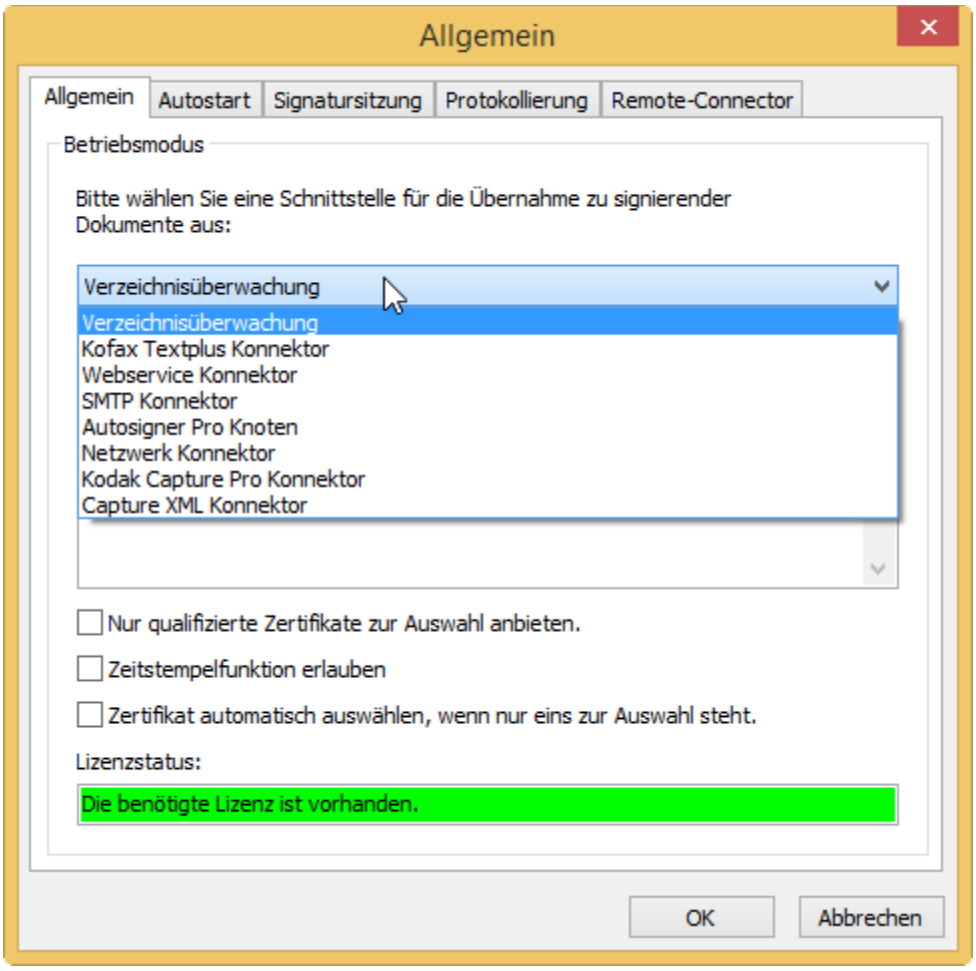

Abbildung 4 – Allgemein.Allgemein

6.2.2 AUTOSTART

Unter " Allgemein -> Autostart" wird entschieden, ob der Signiervorgang automatisch starten soll. Darüber hinaus kann an dieser Stelle festlegt werden, welches Zertifikat der Autosigner beim Programmstart für das Signieren verwenden soll.

Durch ein Klicken auf ‚Anzeigen', werden weitere Informationen zu diesem Zertifikat angezeigt.

Bei SmartCard-Zertifikaten ist eine PIN-Eingabe zwingend erforderlich.

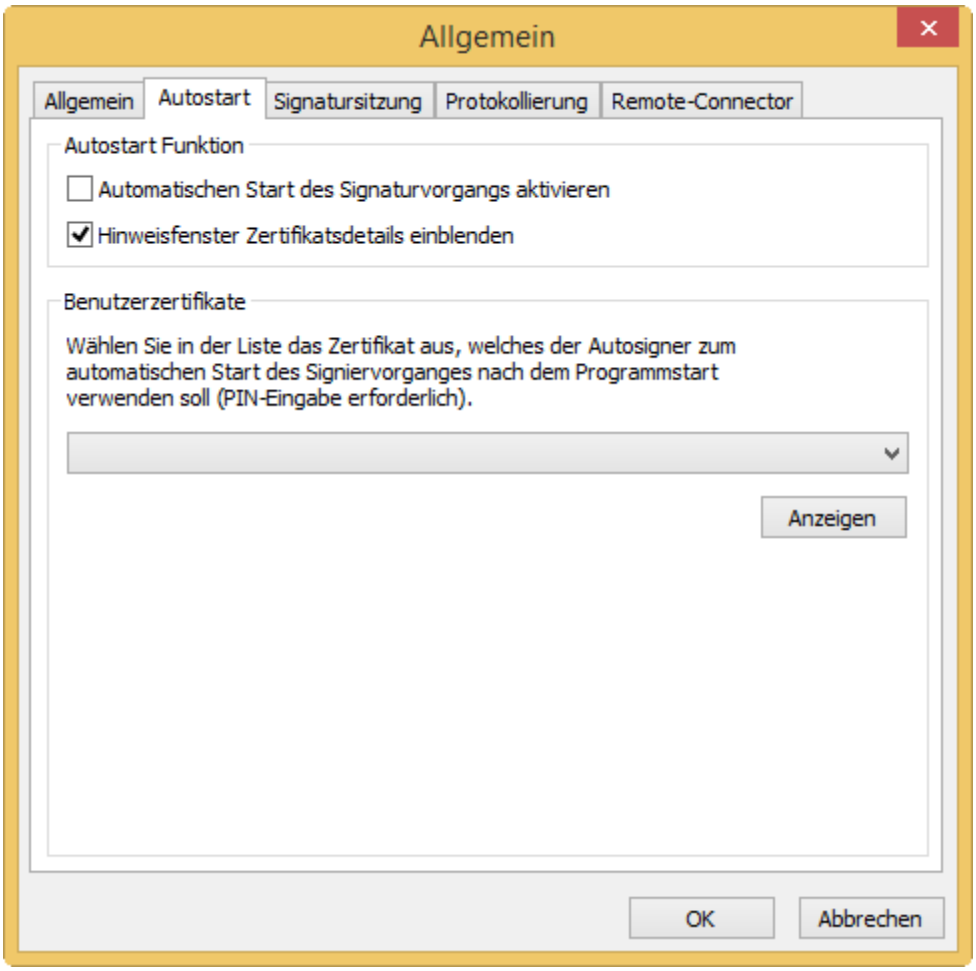

Abbildung 5 – Allgemein.Autostart

6.2.3 SIGNATURSITZUNG

Unter " Allgemein -> Betriebsmodus" kann man die Gültigkeitsdauer der Signatursitzungen konfigurieren.

In der Standardeinstellung wird die Gültigkeitsabfrage nach jeder PIN-Eingabe durchgeführt. Die Gültigkeitsdauer kann jedoch auch individuell über die anderen Optionen angepasst werden. Man kann zwischen unbegrenzt, limitiert auf eine Anzahl von Dokumenten oder limitiert für eine bestimmte Zeitspanne, wählen.

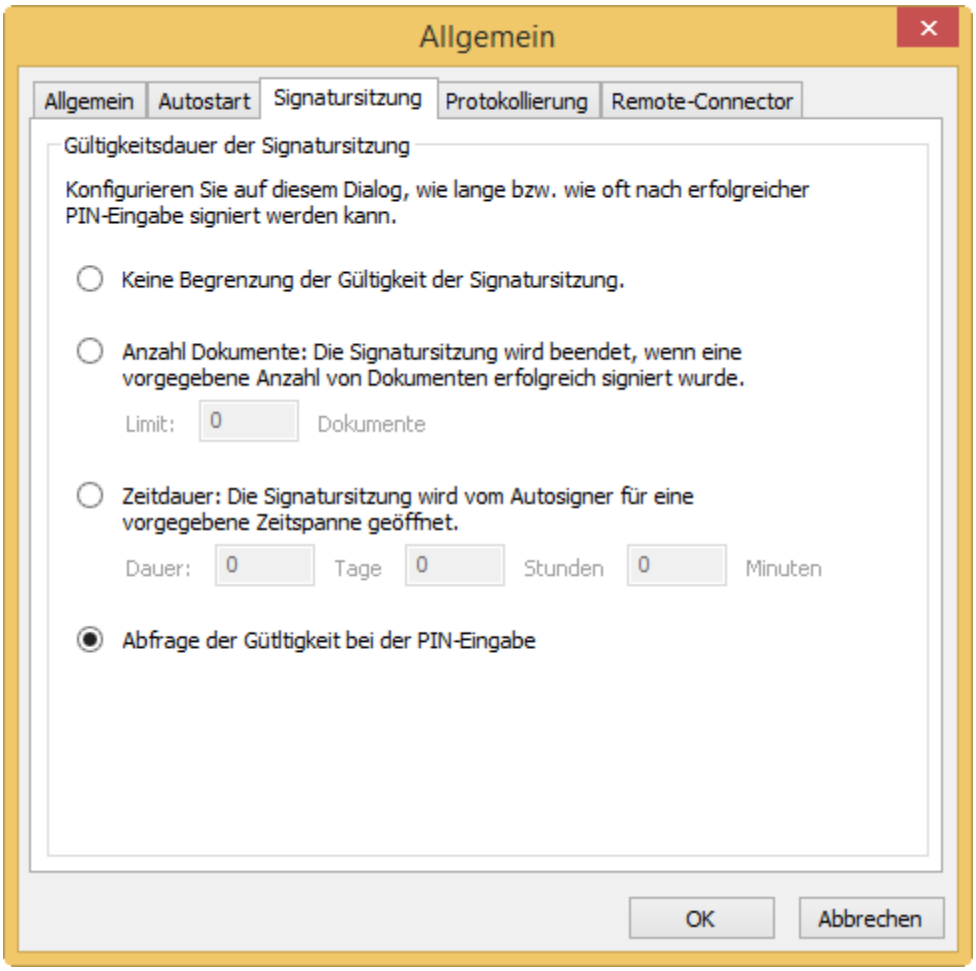

Abbildung 6 – Allgemein.Signatursitzung

6.2.4 PROTOKOLLIERUNG

Unter " Allgemein -> Protokollierung" kann man den Schwellwert für die interne Ereignisverarbeitung festlegen. Standard ist ‚Information'. Zusätzlich kann man den Schwellwert für das Verschicken der Logs an den Administrator auswählen. Standard ist hierbei ‚Fehler'. Für die Ereignisprotokollierung kann man hier einen Protokolldienst wählen und den Speicherort festlegen.

6.2.5 REMOTE-CONNECTOR

Wenn eine Lizens für den Fernzugriff über eine Netzwerkschnittstelle ist der Tab Remote-Connector vorhanden. Hier bestimmen die den Port auf den für den Dienst zur Verfügung steht und welche Benutzer Zugang haben.

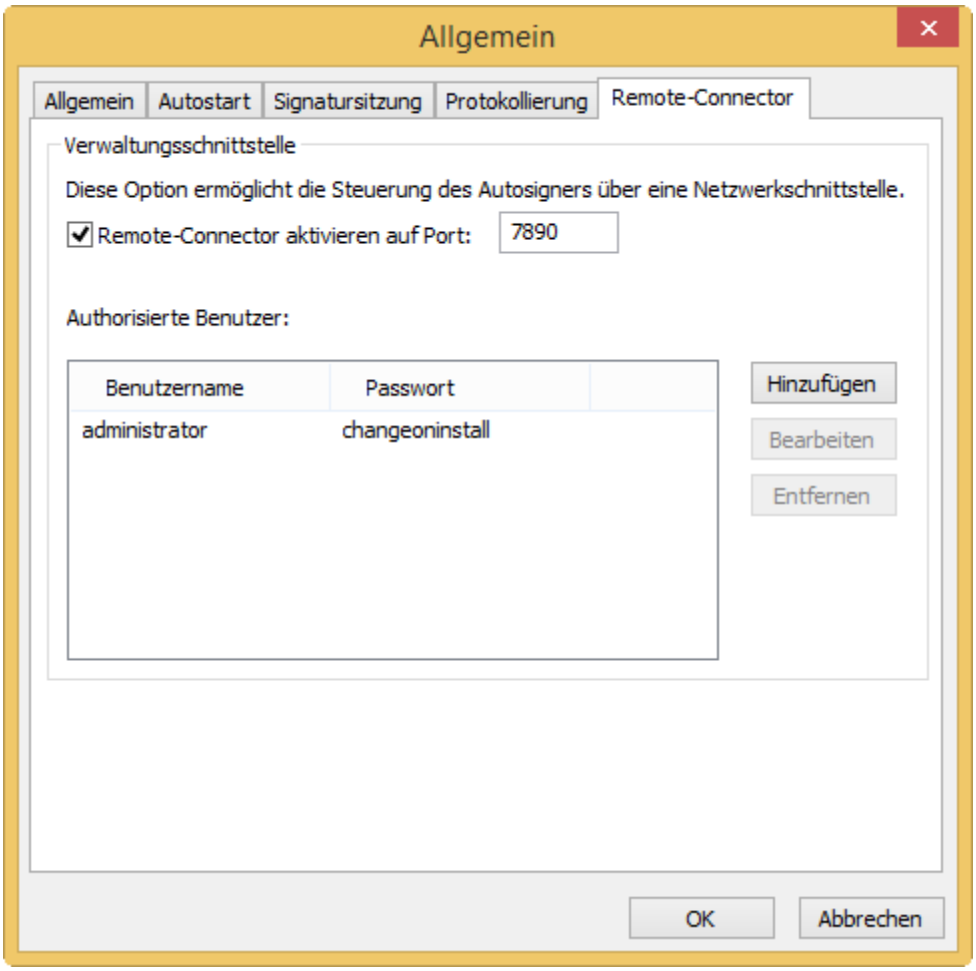

Abbildung 7 – Allgemein.Remote-Connector

6.3 SIGNATUR-EINSTELLUNGEN

Unter "Einstellungen -> Signatur" öffnet sich das Registerkartenfenster zur Konfiguration der Signatur

6.3.1 SIGNATURERSTELLUNG

"Signatur-Einstellungen -> Signaturerstellung" bietet verschiedene Optionen zur Erstellung einer Signatur. ‚Eingebettete PDF-Signatur' bedeutet, dass die Signatur auf dem PDF-Dokument nicht sichtbar ist. ‚Eingebettete, sichtbare PDF-Signatur', lässt die Signatur sichtbar werden. Darüber hinaus kann ein Zeitstempel hinzugefügt werden, welcher Datum und Uhrzeit der PDF-Signatur anzeigt.Wird die ‚Externe Signatur' ausgewählt, werden von allen Dokumenten, die sich im Eingangsverzeichnis befinden eine signierte .p7s-Datei angelegt. Die Original-Datei wird nicht signiert. Image Dateien (TIFF/JPEG) können in ein PDF-Dokument umgewandelt und dann signiert werden. Für XML-Dokumente besteh auch die Möglichkeit einer eingebetteten Signatur. Sonstige Binärdateien werden immer extern signiert. Für jeden Dateityp besteht die Möglichkeit ihn über ‚Ignorieren' von der Signatur auszuschließen.

Es kann eingestellt werden ob eine Integritäsprüfung nach der Signaturerstellung gemacht werden soll.

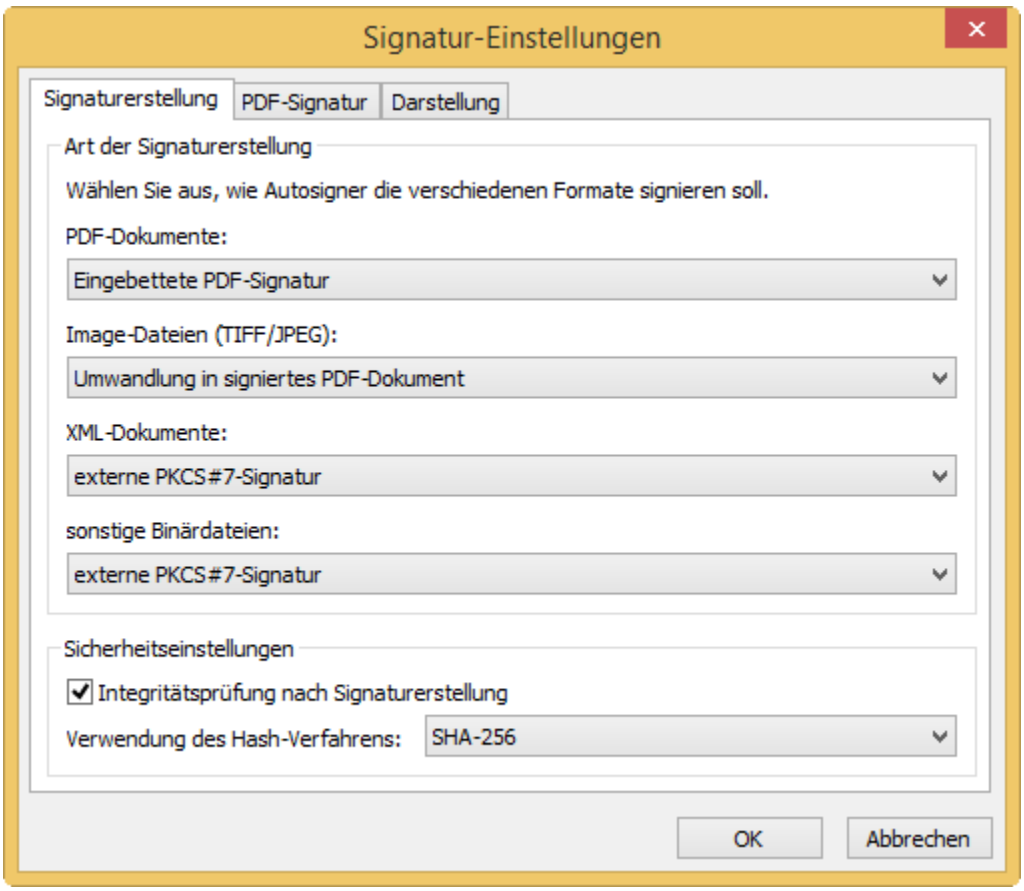

Abbildung 8 – Signatur-Einstellungen.Signaturerstellung

6.3.2 PDF-SIGNATUR

Unter "Signatureinstellung -> PDF-Signatur" können der Signatur zusätzliche Attribute hinzugefügt werden. Dazu zählen: ‚Grund der Dokumentenunterzeichnung', Ort der Signaturerstellung, sowie eventuelle Kontaktinformationen des Unterzeichners.

Zudem kann hier eine URL zu einem Zeitstempel Anbieter angegeben werden.

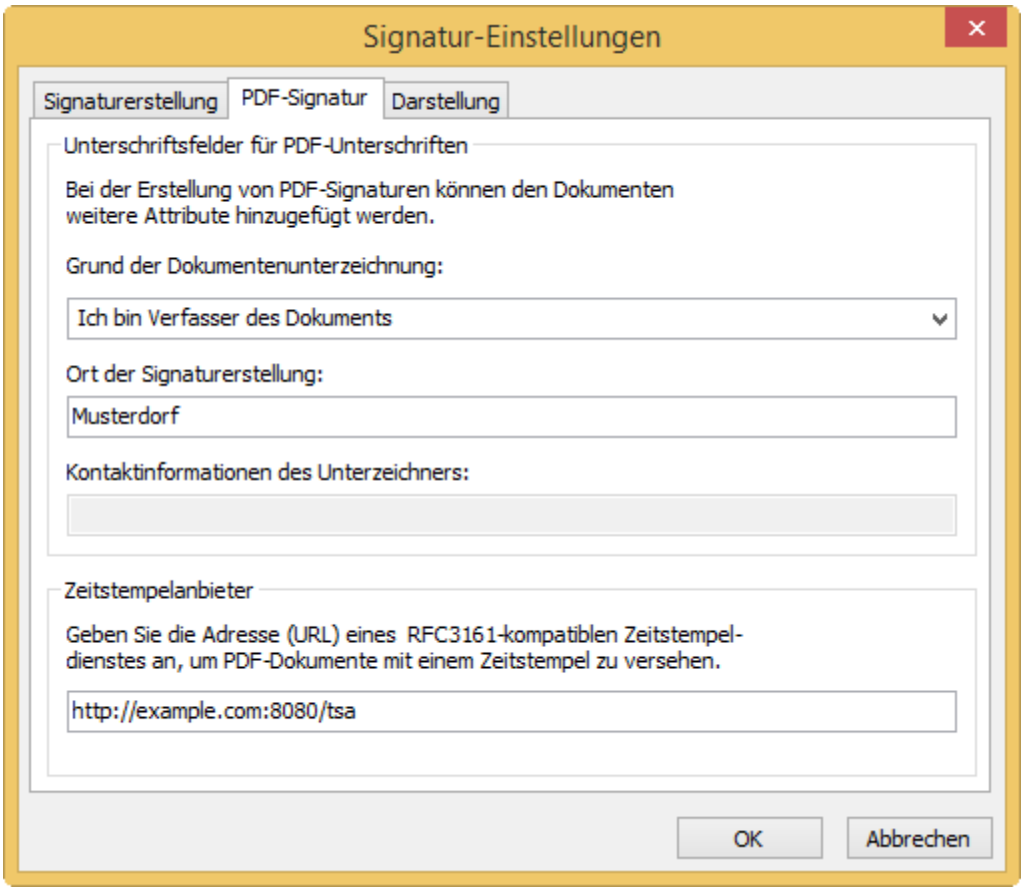

Abbildung 9 – Signatur-Einstellungen.PDF-Signatur

6.3.3 DARSTELLUNG

Unter "Signatur -> Darstellung" kann man das Erscheinungsbild und die Position der Signatur verändern. Ein neue Definitionsdatei (XML-Datei) kann über ‚Hinzufügen' eingefügt werden.

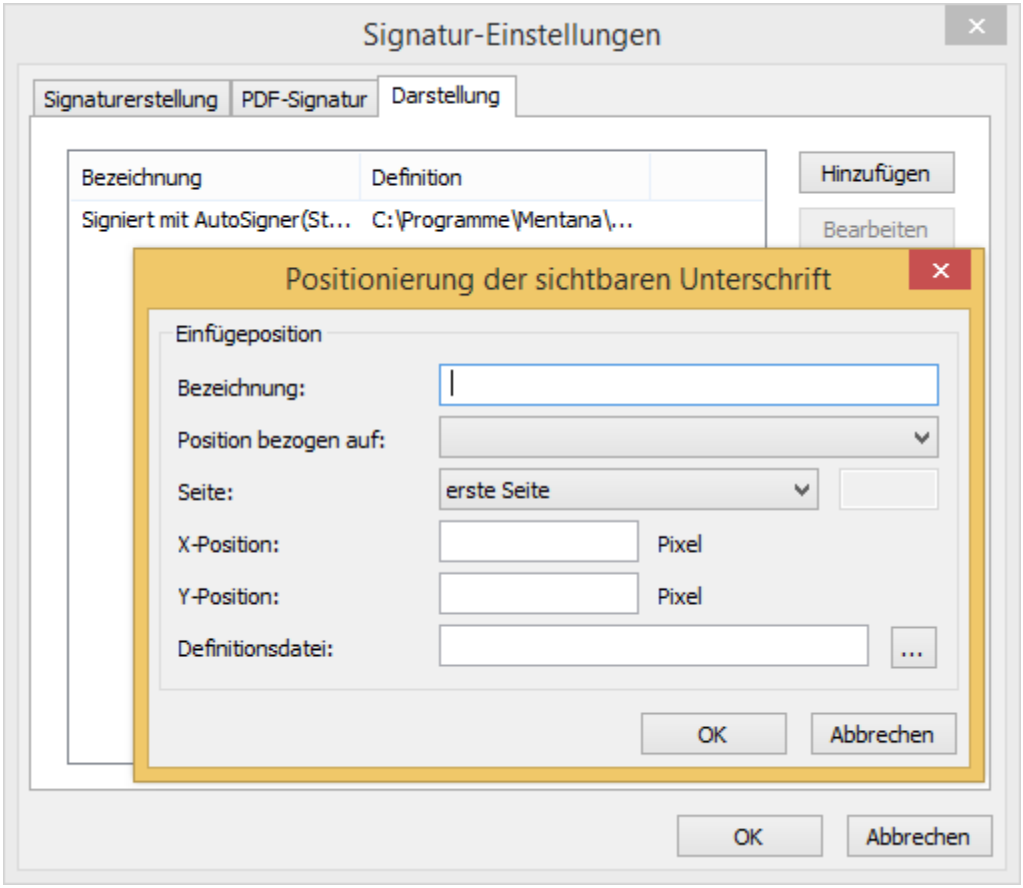

Abbildung 10 – Signatur-Einstellungen.Darstellung – Hinzufügen

6.3.4 LOGOKONFIGURATION

Die Konfiguration der sichtbaren Unterschrift im PDF-Dokument erfolgt mit Hilfe einer XML-Datei. Dort wird festgelegt, wie groß das Signaturfeld sein soll, welche Grafik als Hintergrund verwendet werden soll und welche Signaturinformationen angezeigt werden sollen.

Aufbau der Konfigurationsdatei

Ein Beispiel der Konfigurationsdatei ist in Abbildung 11 zu sehen.

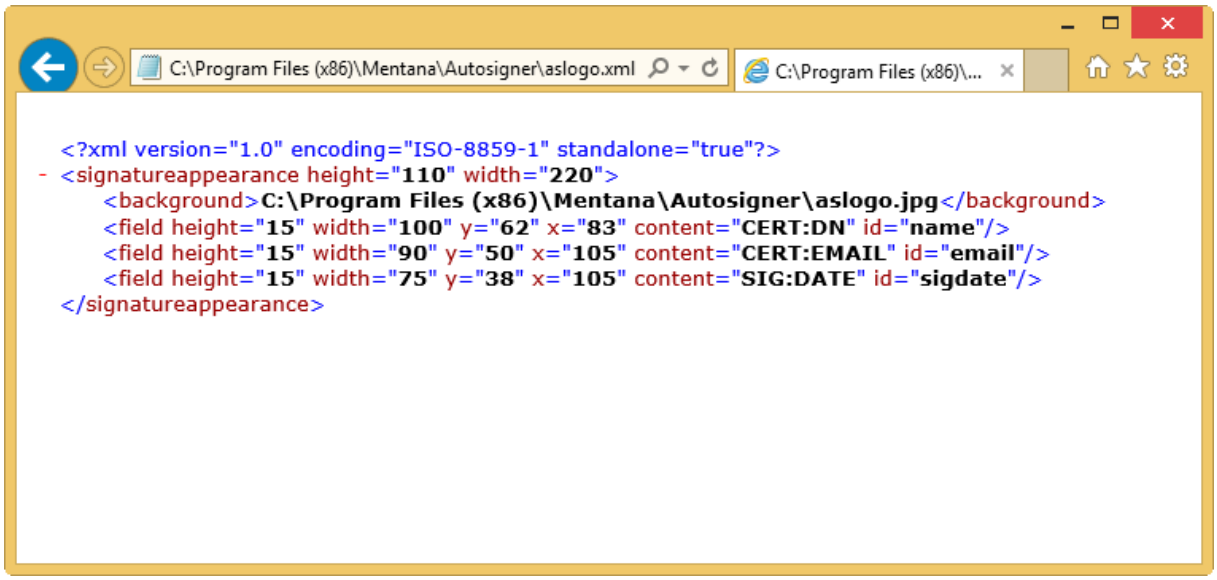

Abbildung 11 – XML-Datei

Die Elemente Einzeln:

<signatureappearance>

Legt das Erscheinungsbild der Signatur fest. Die Eigenschaften **width** und **height** bestimmen die Breite und die Höhe des Signaturfeldes.

<background>

Legt die die Hintergrundgrafik fest, die hinter das Signaturfeld gelegt werden soll.

<field>

Bestimmt die zusätzlichen Informationen, die im Signaturfeld angezeigt werden sollen. Die Eigenschaft **id** legt einen eindeutigen Namen des Feldes fest. Dieser ist frei wählbar. Mit Hilfe der Eigenschaft **content** bestimmt man, welche Daten auf dem Signaturfeld angezeigt werden sollen. Es können folgende Werte verwendet werden.

- CERT:DN: Zertifikat ausgestellt für
- CERT:SERIAL: Zertifikat Seriennummer
- CERT:ISSUER: Zertifikat Aussteller
- CERT:ORG: Zertifikat Organisation
- CERT:OU: Zertifikat Organisationseinheit
- CERT:EMAIL: Zertifikat E-Mail
- CERT:FINGERPRINT: Zertifikat Fingerabdruck
- SIG:DATE: Datum / Zeit der Unterschrift
- SIG:REASON: Grund der Unterschrift
- SIG:LOCATION: Ort der Unterschrift

Die Eigenschaften **width**, **height**, **x**, **y** legen die Größe und die Position des Feldes innerhalb des Signaturfeldes fest. Der Bezugspunkt für **x** (vertikale Achse) und **y** (horizontale Achse) ist die linke untere Ecke des Signaturfeldes.

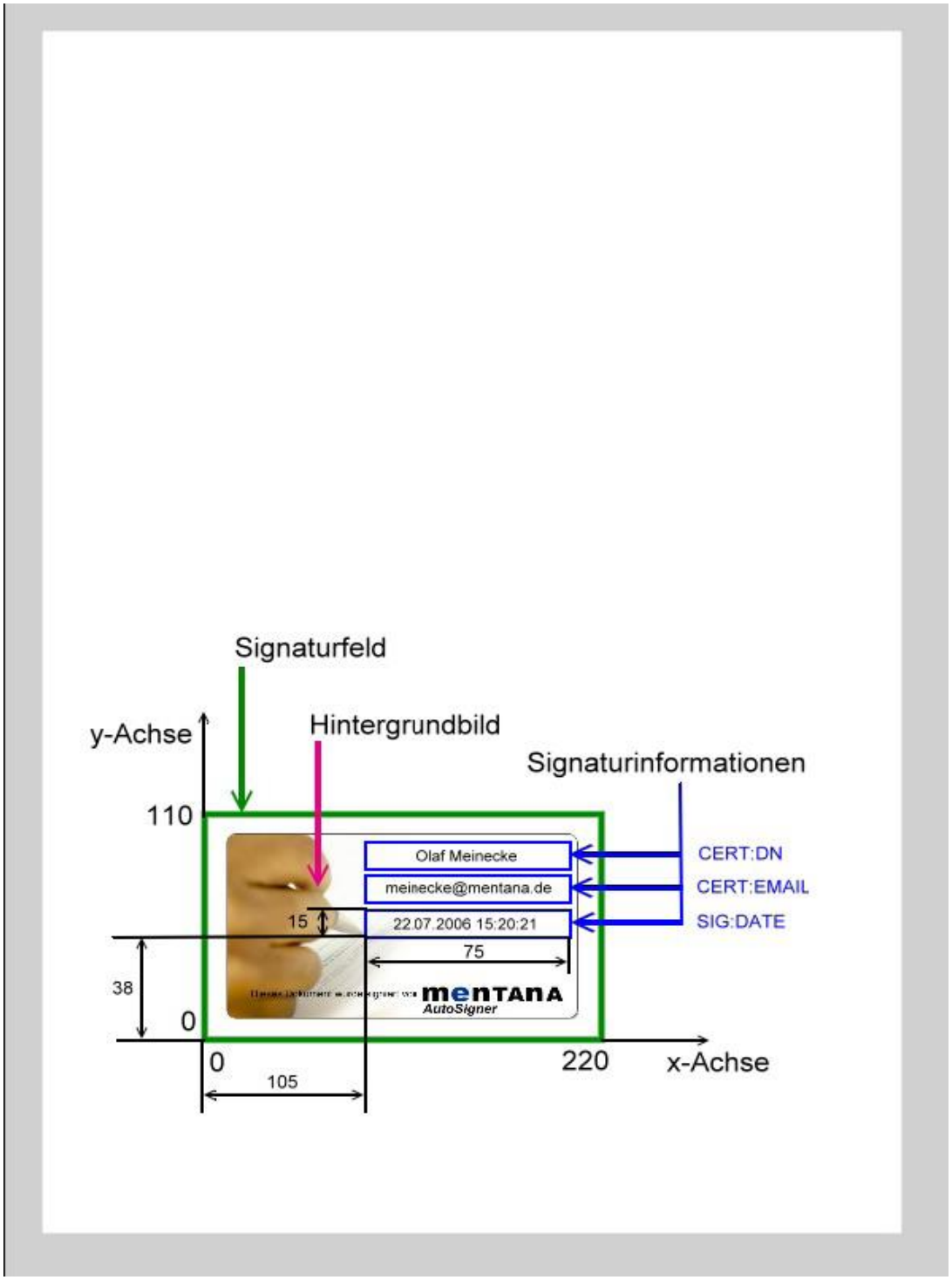

Abbildung 12 – Positionierung

6.4 VERZEICHNISÜBERWACHUNG

Unter "Einstellungen -> Verzeichnisüberwachung" öffnet man das Registerkartenfenster zur Verzeichnisüberwachung. An dieser Stelle wird festgelegt aus welchem Verzeichnis der AutoSigner die zu signierenden Dokumente beziehen soll und wo er im Anschluss die erfolgreich signierten Dokumente ablegen wird.

Ein Verzeichnis für Sicherheitskopien (Backups) und ein Verzeichnis für Fehlermeldungen kann ebenfalls angegeben werden.

6.4.1 ALLGEMEIN

Unter "Verzeichnisüberwachung -> Allgemein" können die Verzeichnisse für die Eingabe von Dokumenten, die Ausgabe von erfolgreich signierten Dokumenten, die Ausgabe von fehlerhaft signierten Dokumenten und für Sicherheitskopien der Eingangsdokumente festgelegt werden. Unter ‚Erweitert' kann festgelegt werden, ob Sicherheitskopien erstellt werden sollen und ob zusätzlich auch Unterverzeichnisse des Eingangsverzeichnis durchsucht werden sollen. Diese Verzeichnisstruktur befindet sich dann auch im angegebenen Ausgangsverzeichnis. Dies bietet bei einer großen Anzahl von Dokumenten eine bessere Übersicht.

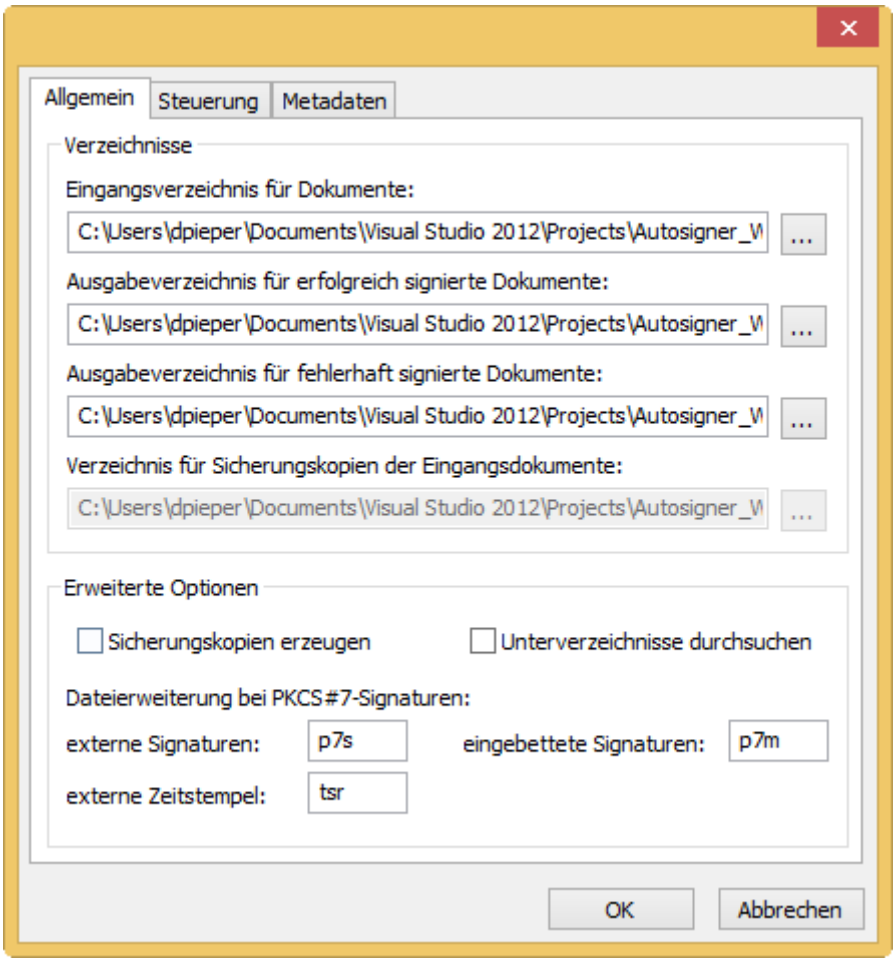

Abbildung 13 – Verzeichnissüberwachung.Allgemein

6.4.2 STEUERUNG

Unter "Verzeichnisüberwachung -> Steuerung" findet man die Einstellungen bezüglich der Sichtprüfung zufällig ausgewählter Dokumente. Eine Stichprobenprüfung kann unter dieser Option aktiviert werden. Zudem kann man den Dokumententyp für das automatische Öffnen hinzufügen. Eine weite Option ist die Auswahlwahrscheinlichkeit, welche in % festzulegen ist. Die Suchprozesspriorität kann hier ebenfalls in Sekunden festgelegt werden. Diese Funktionen dienen einer besseren Sicherheit für das Signieren von Dokumenten.

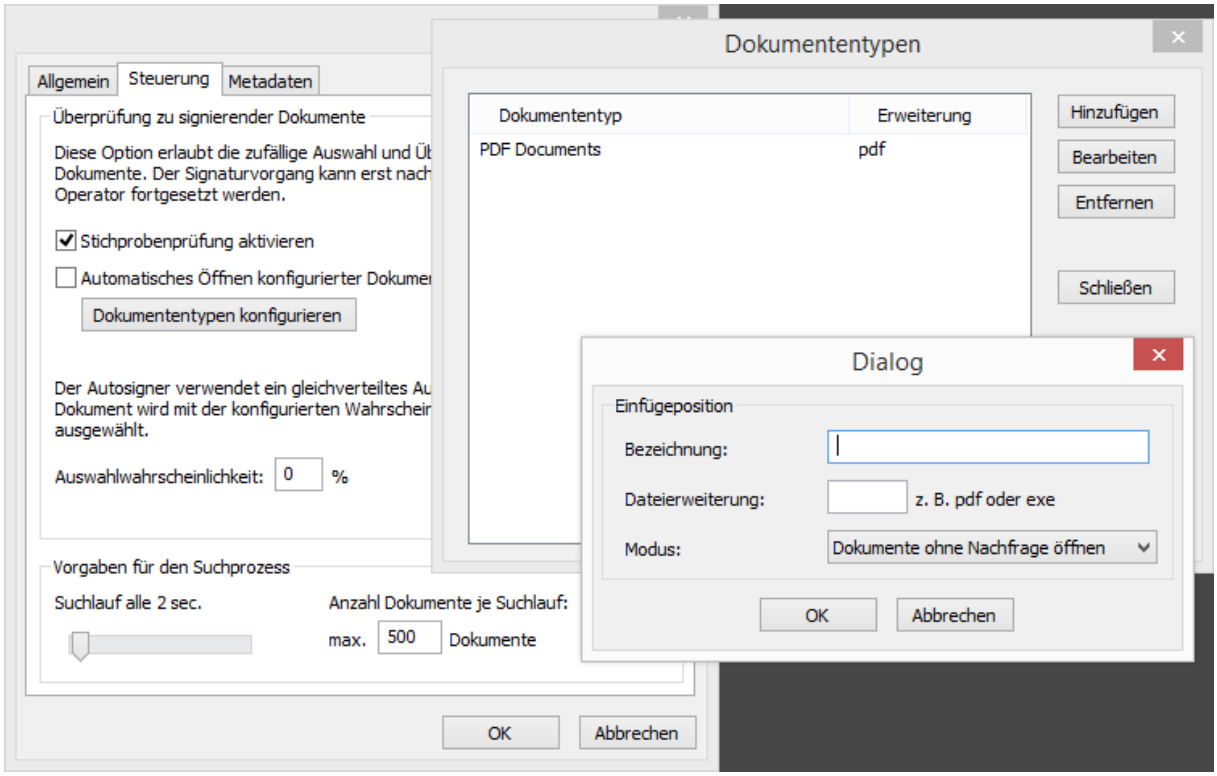

Abbildung 14 – Verzeichnissüberwachung.Steuerung – Dokumenttypen konfigurieren

6.5 STARTEN, UNTERBRECHEN, ABBRECHEN EINER SIGNATUR

Man kann die einen Signaturvorgang auf zweierlei Art und Weise starten, unterbrechen und abbrechen.

Eine Möglichkeit bietet der Menüpunkt ‚Datei' in der Menuleiste. Bei einem Klick auf diese Schaltfläche öffnet sich ein Popup-Fenster, mit dem man die gewünschte Aktion ausführen kann.

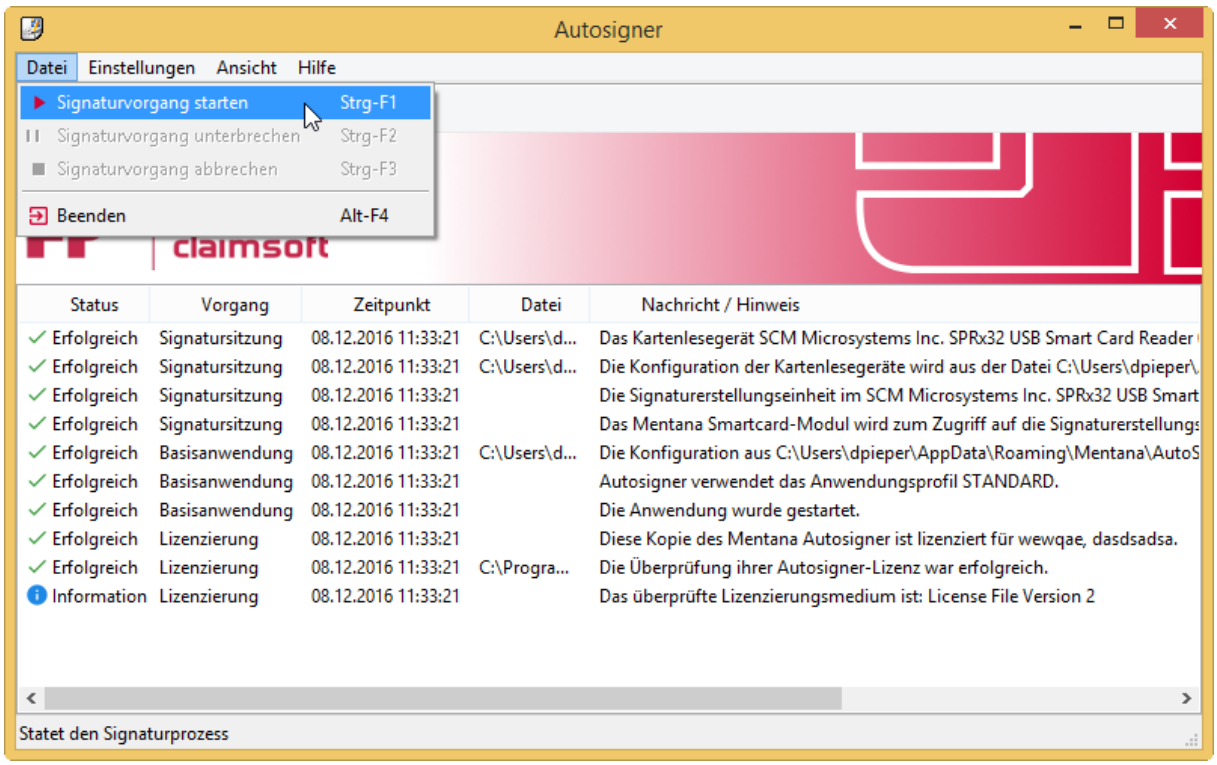

Abbildung 15 – Signaturvorgang starten

Die zweite Variante mit der man einen Signaturvorgang beeinflussen kann, bietet die Toolleiste unter der Menuleiste.

Man kann durch einen einfachen Klick den Signaturvorgang starten, unterbrechen und abbrechen. Darüber hinaus bietet diese Leiste zwei weitere Buttons. Einer bietet eine Funktion die komplette Ereignisanzeige zu löschen, der andere ruft ein ‚About Mentana AutoSigner'-Dialogfenster auf.

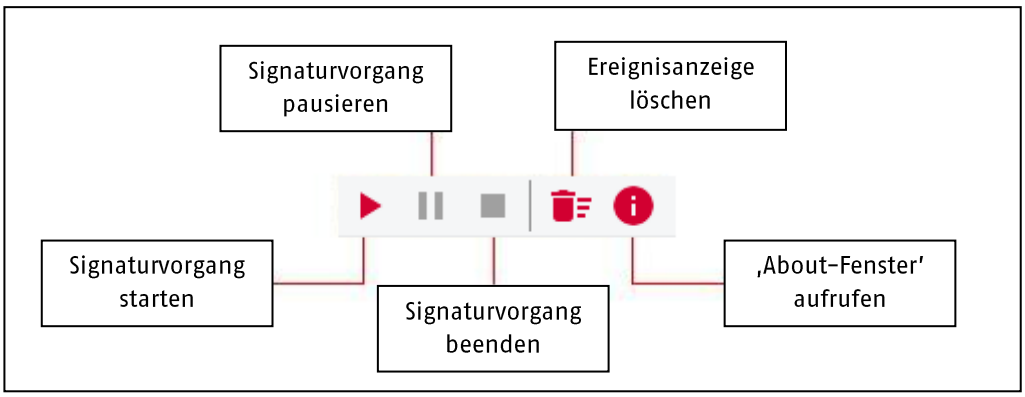

Abbildung 16 – Toolleiste

Wird der Signaturvorgang gestartet erscheint folgendes Fenster:

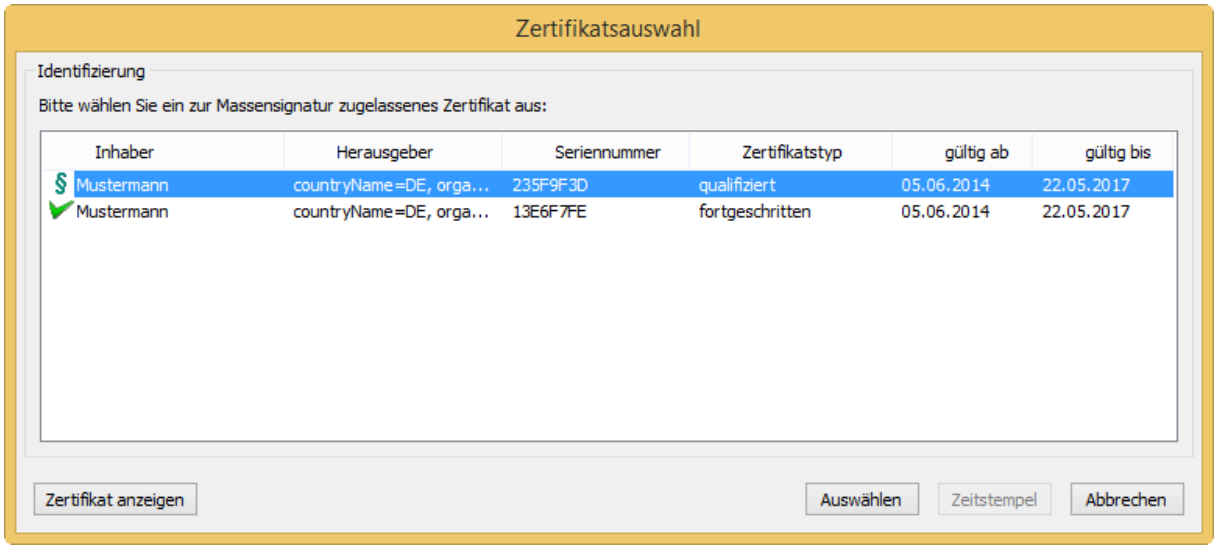

Abbildung 17 – Zertifikat wählen

Hier kann man das Zertifikat wählen, welches zum Signieren eines Dokuments genutzt werden soll.

Über den Button 'Anzeigen' ist es möglich, sich die Details zu einem Zertifikates anzeigen zulassen. Der Signaturvorgang startet durch Anklicken von 'OK'.

Es werden die im Eingangsverzeichnis vorhandene PDF-Dokumente je nach ausgewähltem Modus sofort oder später signiert.

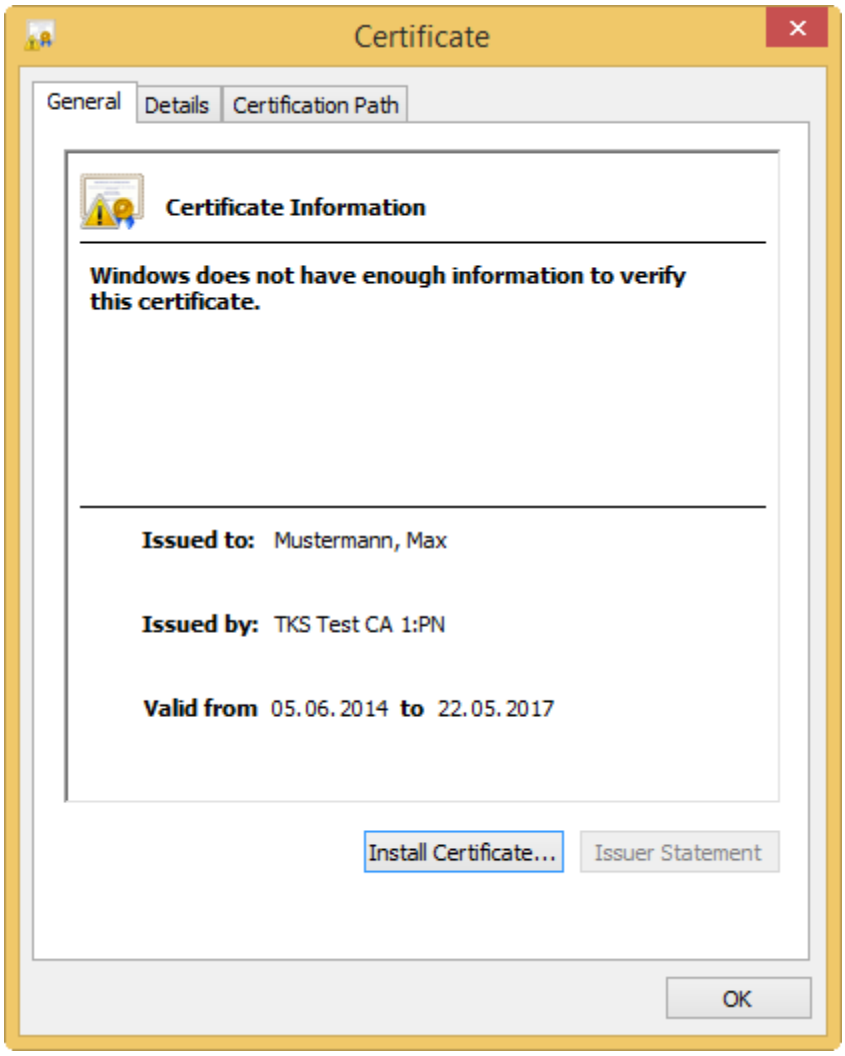

Abbildung 18 – Anzeige des Zertifikates

Hinweis:

Ist der Signaturvorgang gestartet, können die Einstellungen nicht mehr geändert werden. Erst nach Ende des Signaturvorganges ist der Menüpunkt "Einstellungen" wieder zugänglich.

6.6 ANWENDUNG SCHLIESSEN

"Datei- > Beenden" beendet den ‚AutoSigner'.

6.7 DATEISYNCHRONISATION

Im laufenden Betrieb kann es zu Fehlern bei der Dateibearbeitung kommen. Es sind folgende Fehlerquellen möglich:

- Es wird versucht einen Signaturvorgang zu starten, während Dokumente in das Eingangsverzeichnis kopiert oder aus dem Ausgangsverzeichnis abgeholt werden.
- Während eines Signaturvorgangs sollen Dokumente in das Eingangsverzeichnis eingefügt werden bzw. aus dem Ausgangsverzeichnis abgeholt werden.

Um diese Fehler zu vermeiden, wurde der folgende Synchronisationsmechansimus implementiert: Wird vom ‚AutoSigner' vor einem Signaturdurchlauf im Eingangsverzeichnis eine Datei *.upload* oder im Ausgangsverzeichnis eine Datei *.download* gefunden, wird der Signaturvorgang nicht gestartet, da diese Dateien signalisieren, dass in den entsprechenden Verzeichnissen im Augenblick Dateioperationen stattfinden. Der ‚AutoSigner' versucht dann in Zeitabständen von fünf Minuten, erneut einen Signaturdurchlauf zu starten. Dieses wiederholt sich bis die *.upload* und/oder die *.download* Datei gelöscht wurde.

Wird vom AutoSigner ein Signaturdurchlauf gestartet, wird im Eingangs- und Ausgangsverzeichnis je eine Datei mit Namen *.running* erstellt. Nach Beendigung des Signaturlaufs werden diese Dateien wieder gelöscht.

Hinweis:

Ein externer Upload- bzw. Downloadprozess ist selbst für das Erstellen der Dateien *.upload* und *.download* vor Dateitransfer und Löschen dieser Dateien nach Dateitransfer zuständig. Diese Prozesse müssen auch überprüfen, ob eine Datei *.running* existiert und ggf. Warten bis diese Dateien gelöscht wurden.

6.8 SMARTCARD-MODUL

Der AutoSigner enthält ein kryptographisches Servicemodul, mit dem Signaturerstellungseinheiten ohne zusätzliche Software des Herstellers angesprochen werden können. Alternative kann auch der Windows-Zertifikatsspeicher ausgewählt werden, wofür allerdings eine CSP notwendig ist.

Kartenlesegerät

Ermöglicht die auswahl des Kartenlesegeräts welches der Autosigner verwenden soll. Zusätzlich kann man die Zertifikate anzeigen lassen welche im jeweiligen Gerät vorhanden sind.

Logging

Zum an und ausschalten der Protokollierung zum Kartenlesegerät und Smarcard. Wieviel protokolliert werden soll kann man im Detaillevel auswählen (0 = Protokollierung aus, 9 = Volle Details).

Fortgeschrittener Modus

Aktiviert/Deaktiviert den fortgeschittenen Modus. Im fortgeschrittenen Modus wird die eingabe der PIN nicht über das PIN-Pad des Kartenlesegrätes durchgeführt sondern üder die Autosigner-Oberfäche per Tastatur.

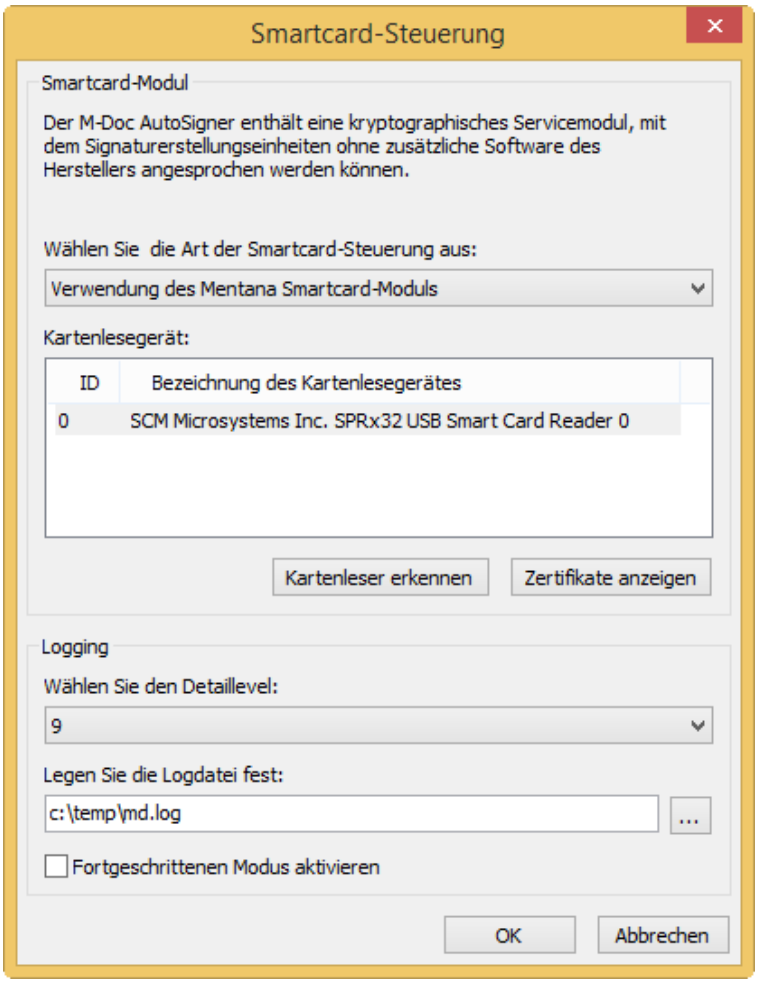

Abbildung 19 – Einstellungen Smartcard-Steuerung

7 DIE KONFIGURATIONSDATEI

Die Konfigurationsdatei liegt ‚config.xml' standardmäßig in "c:\Dokumente und Einstellungen\%USERNAME%\Anwendungsdaten\Mentana\AutoSigner." Diese Datei kann aber über den Kommandoparameter "/configfile=Dateiname" bei Aufrufung des AutoSigners umgeändert werden.

8 LOGDATEIEN

Die erfolgreich durchgeführten Signaturvorgänge sowie Meldungen über aufgetretene Fehler werden in Logdateien mitgeschrieben. Die entsprechenden Meldungen werden in die jeweils aktuelle Logdatei geschrieben, wobei für jeden Tag eine neue Logdatei angelegt wird. Die Syntax des Dateinamens einer Logdatei lautet dabei *autosigner-DD-MM-YYYY.txt* (etwa autosigner-15-09-2016.txt). Das Verzeichnis für die Logdateien ist unter "Bearbeiten -> Einstellungen -> Allgemein -> Protokollierung" auszuwählen oder zu ändern. Es können der Logdatei die nachfolgenden Informationen entnommen werden:

- Die Kopfzeile wird in dieser Form angezeigt:
  ---------- Logfile created / reopened on DD.MM.YYYY HH:MM:SS ----------
- Start des Signaturvorgangs nicht möglich (HASP-Key Abfrage). → Ausgabe eines Fehlercodes (siehe 8.2.3).
- Info über den Start eines Signaturvorgangs.
- Welche Datei wurde signiert?
- Das Signieren einer Datei war erfolgreich oder ist fehlgeschlagen. → Ausgabe eines Fehlercodes (siehe 8.2.2).
- Abbruch des Signaturvorgangs (HASP-Key Abfrage: HASP-Key wurde z.B. während Betrieb entfernt). → Ausgabe eines Fehlercodes (siehe 8.2.3).
- Info über den Abschluss eines Signaturvorgangs.
- Weitere:
  - eine zu signierende Datei ist bereits im Ausgangsverzeichnis vorhanden.
  - der Schreibschutz einer Datei wurde entfernt.
  - eine Datei konnte nicht gelöscht werden.
  - Dokument beinhaltet unbekanntes Seitenformat (bei sichtbarer Signierung)

8.1 AUSZUG AUS EINER LOGDATEI

```
--------------- Logfile created / reopened on 15.09.2015 10:55:28 --------------------

15.09.2015 10:55:28 [SUCCESS] [Basisanwendung]

Message: Die Anwendung wurde gestartet.

15.09.2015 10:55:28 [SUCCESS] [Lizenzierung]

Message: Die Überprüfung ihrer Autosigner-Lizenz war erfolgreich.

15.09.2015 10:55:28 [SUCCESS] [Lizenzierung]

Message: Diese Kopie des Mentana Autosigner ist lizenziert für Testlizenz, Mentana-Claimsoft
AG.

15.09.2015 10:55:46 [SUCCESS] [Signatursitzung]

Message: Zertifikat Wiege Sebastian (SN: 28A3DA2400000000001B) zum Signieren ausgewählt.

15.09.2015 10:55:47 [SUCCESS] [Basisanwendung]

Message: Eine Signaturinstanz vom Typ Dateisystemscanner wurde erzeugt und initialisiert.

15.09.2015 10:55:47 [SUCCESS] [Signatursitzung]

Message: Die sichere Signatursitzung wurde erfolgreich eröffnet.

15.09.2015 10:55:47 [SUCCESS] [Signatursitzung]

Message: Die Laufzeit der Signatursitzung wird nicht begrenzt.

15.09.2015 10:55:47 [SUCCESS] [Vorverarbeitung]

File: C:\Programme\Mentana\Autosigner\in\vcpp6.pdf

Message: Eine Kopie der Ursprungsdatei wurde vor Anbringen der Signatur im Backupverzeichnis
angelegt.

15.09.2015 10:55:47 [ERROR] [Signatur]

File: C:\Programme\Mentana\Autosigner\in\vcpp6.pdf

Message: Sichtbare Signatur fehlgeschlagen. (unbekanntes Seitenformat)

15.09.2015 10:55:47 [INFORMATION] [Signatur]

File: C:\Programme\Mentana\Autosigner\in\vcpp6.pdf

Message: Das Dokument wird ersatzweise mit einer einfachen, eingebetteten PDF-Signatur
versehen.

15.09.2015 10:55:48 [SUCCESS] [Signatur]

File: C:\Programme\Mentana\Autosigner\in\vcpp6.pdf

Message: Signaturerstellung erfolgreich, Verarbeitungszeit 304.65 ms.

15.09.2015 10:56:03 [INFORMATION] [Signatursitzung]

Message: Die sichere Signatursitzung wurde geschlossen, der Signaturvorgang ist beendet.

--------------- Logfile created / reopened on 15.09.2015 11:17:03 --------------------

15.09.2015 11:17:04 [SUCCESS] [Basisanwendung]

Message: Die Anwendung wurde gestartet.
```

```
15.09.2015 11:17:04 [ERROR] [Lizenzierung]

Message: Ihre Autosigner-Lizenz konnte nicht erfolgreich überprüft werden. Bitte wenden Sie
sich an support@mentana.de

15.09.2015 11:17:12 [SUCCESS] [Signatursitzung]

Message: Zertifikat Wiege Sebastian (SN: 28A3DA2400000000001B) zum Signieren ausgewählt.

15.09.2015 11:17:14 [ERROR] [Signatursitzung]

Message: Ihre Autosigner-Lizenz konnte nicht erfolgreich überprüft werden. Bitte wenden Sie
sich an support@mentana.de
```

8.2 FEHLERCODES

Im Folgenden sind die möglichen Fehlercodes aufgelistet, die bei der Ausführung des ‚Autosigners' innerhalb der Anwendung zurückgeliefert und in einer Logdatei ausgegeben werden.

8.2.1 ALLGEMEINE FEHLER

Bei einem allgemeinen Fehler wird ein Wert ungleich 0 zurückgeliefert, etwa bei einem internen Verarbeitungsfehler.

8.2.2 SIGNATURCODES (MDOCAPI-FEHLERCODES)

Fehlercode hex (dez)	Defines	Erläuterung
0x0 (0)	OK	Operation erfolgreich durchgeführt.
0xFFFFFFFF (-1)	ERROR_CAN_NOT_LOAD_PDF_FILE	PDF-Datei kann nicht geladen werden
0xFFFFFFFE (-2)	ERROR_START_XREF	XREF-Tabelle kann nicht gefunden werden
0xFFFFFFFD (-3)	ERROR_POS_TRAILER	Trailer kann nicht gefunden werden
0xFFFFFFFC (-4)	ERROR_READING_KEY_VAL_GENERAL	Schlüsselwert im PDF-Dokument wird nicht gefunden
0xFFFFFFFB (-5)	ERROR_CAN_NOT_CREATE_COPY	Kopie kann nicht erstellt werden
0xFFFFFFFA (-6)	ERROR_NO_CERTIFICATE_IN_STORE	Kein Zertifikat im Store
0xFFFFFFF9 (-7)	ERROR_INPUT_TO_LONG	Eingabe zu lang
0xFFFFFFF8 (-8)	ERROR_ON_INPUT	Fehlerhafte Parameterangabe
0xFFFFFFF7 (-9)	ERROR_TIMESTAMP_BINDING	Z.Zt. nicht verwendet
0xFFFFFFF6 (-10)	ERROR_TIMESTAMP_CONFIG	Fehler beim Konfigurieren des Zeitstempels
0xFFFFFFF5 (-11)	ERROR_MAKING_TIMESTAMP	Fehler beim Erstellen des Zeitstempels
0xFFFFFFF4 (-12)	ERROR_OPENING_FILE	Fehler beim Dateiöffnen
0xFFFFFFF3 (-13)	ERROR_READ_FIELDS	Fehler beim Lesen der Felder
0xFFFFFFF2 (-14)	ERROR_CANNOT_OPEN_INI_FILE	Ini-Datei kann nicht geöffnet werden

0xFFFFFFF1 (-15)	ERROR_CANNOT_CLONE_PDF	PDF-Datei kann nicht geklont werden.
0xFFFFFFF0 (-16)	ERROR_READING_FIELDS	Z.Zt. nicht verwendet
0xFFFFFFEF (-17)	ERROR_READ_INI_FILE	Fehler beim Lesen der ini-Datei.
0xFFFFFFEE (-18)	ERROR_READ_TRAILER	Trailer kann nicht gelesen werden
0xFFFFFFED (-19)	ERROR_APPEND_OBJ	Z.Zt. nicht verwendet
0xFFFFFFEC (-20)	ERROR_WRITE_TRAILER	Fehler beim Schreiben des Trailers
0xFFFFFFEB (-21)	ERROR_ENCRYPTED_PDF_FILE	Fehler beim Verschlüsseln der PDF-Datei
0xFFFFFFEA (-22)	ERROR_VISIBLE_SIG_NOT_POSSIBLE	Sichtbare Signatur nicht möglich.
0xFFFFFFE9 (-23)	ERROR_CREATE_SIGNED_PDF	Fehler beim Erstellen der signierten PDF-Datei
0xFFFFFFE8 (-24)	ERROR_WRITE_SIGNED_PDF	Fehler beim Signieren der internen Nachricht (z.B. beim fehlerhaften Zugriff auf den privaten Schlüssel)
0xFFFFFFE7 (-25)	ERROR_NO_CONTENT_TO_SIGN	Keine Nachricht zum Signieren vorgefunden. (z.B. eine leere Datei)
0xFFFFFFE6(-26)	ERROR_CREATE_PDF_ATTACHMENT	Fehler beim Hinzufügen von Dateianlagen
0xFFFFFFE5(-27)	ERROR_VISIBLE_FIELD_NOT_POSSIBLE	Erstellen eines sichtbaren Unterschriftfeldes nicht möglich
0xFFFFFFE4 (-28)	ERROR_OPENING_GRAPHICS_FILE	Fehler beim Öffnen der Grafik-Datei
0xFFFFFFE2 (-30)	ERROR_IDENTICAL_FILES_4_DETACHED_SIG	Identischer Dateiname für die Signatur
0xFFFFFFE1 (-31)	ERROR_SIGNATURE_FILE_EXISTS	Signaturdatei existiert
0xFFFFFFE0 (-32)	ERROR_CAN_NOT_CREATE_SIGFILE	Fehler beim Erstellen der Signaturdatei

0xFFFFFFDA (-38)	ERROR_WRITE_PDF_FILE	Fehler beim Unterschreiben der PDF-Datei
0xFFFFFFD8 (-40)	ERROR_INCORRECT_DATE_FORMAT	Falsches Datum Format
0xFFFFFFB0(-80)	ERROR_MEMORY_ALLOCATION	Fehler beim Speicherreservieren
0xFFFFFFAF (-81)	ERROR_READING_FILE	Datei kann nicht gelesen werden
0xFFFFFF9F (-97)	ERROR_SIGN_13	Z.Zt. nicht verwendet
0xFFFFFF9E (-98)	ERROR_IMAGE	Z.Zt. nicht verwendet
0xFFFFFF9D (-99)	ERROR_DISTILLER	Z.Zt. nicht verwendet
0xFFFFFF55 (-171)	ERROR_OPENING_ATTACHING_FILE	Fehler beim Öffnen der Datei für den Datenanhang
0xFFFFFF54(-172)	ERROR_NO_CONTENT_TO_ATTACH	Keinen Inhalt für den Datenanhang gefunden
0xFFFFFF53 (-173)	ERROR_FILE_EXT_NOT_SUPPORTED	Datei wird nicht unterstützt
0xFFFFFF21 (-801)	ERROR_SETTING_TJ_VALUE	Fehler beim Ausfüllen der Formularfelder

Tabelle 1 – MDocAPI Fehlercodes

Die einzelnen Fehlercodes werden je nach Prüfart bzw. wenn mehrere Fehler auftreten auch verodert zurückgeben.

8.2.3 HASP-FEHLERCODES

Fehlercode (dez)	Erläuterung
0	Vorgang erfolgreich.
-1	Timeout: Schreibvorgang nicht erfolgreich.
-2	Adresse außerhalb des zulässigen Bereichs.
-3	Ein HASP-Key mit dem angegebenen Passwort wurde nicht gefunden.
-4	Ein HASP-Key wurde gefunden, aber es ist kein HASP-Key mit Speicher.
-5	Schreibvorgang nicht erfolgreich.
-6	Der parallele Port ist zur Zeit nicht verfügbar. Ein anderes angeschlossenes Gerät, z.B. ein Drucker, ist gerade aktiv. Wiederholen Sie den Aufruf nach einigen Sekunden.
-7	Der Puffer ist nicht groß genug. Dieser Fehler tritt nur bei Diensten auf, die eine Untergrenze für die Puffergröße haben.
-8	Die Hardware unterstützt den gewünschten Dienst nicht. Dieser Dienst erfordert, dass ein HASP4-Key angeschlossen ist.
-9	Ungültiger Zeiger. Der an den Dienst übergebene Zeiger ist nicht gültig.
-10	Zugriff auf den Key verweigert, weil die Anwendung auf einem Netzwerk-Monitor über Citrix Winframe oder Windows Terminal Server betrieben wird. Die Anwendung kann nur auf dem Konsolenmonitor selbst betrieben werden.
-11	Zugriff auf den Key verweigert, weil die Anwendung auf einem Netzwerk-Monitor über Citrix Winframe oder Windows Terminal Server betrieben wird. (Servicepack 4+ ist erforderlich, um festzustellen, ob sie auf dem Konsolenmonitor läuft.)
-12	Ein an den Dienst übergebener Parameter ist nicht gültig oder außerhalb des zulässigen Bereichs.
-13	Falsche Version. Diese Fehlermeldung zeigt an, dass der Treiber zu alt ist für die API. Sie sollten Ihren Treiber aktualisieren. Dies gilt nur für Win32- und Win64-Anwendungen.
-100	HASP-Gerätetreiber kann nicht geöffnet werden. Installieren Sie den HASP-Gerätetreiber.
-110	HASP-Gerätetreiber kann nicht geöffnet werden. Bei DOS-, DOS-Extender- und Win16-Anwendungen, die auf den HASP-Gerätetreiber zugreifen. Installieren Sie den HASP-Gerätetreiber.
-111	HASP-Gerätetreiber kann nicht gelesen werden. Bei DOS-, DOS-Extender- und Win16-Anwendungen, die auf den HASP-Gerätetreiber zugreifen.

-112	HASP-Gerätetreiber kann nicht geschlossen werden. Bei DOS-, DOS-Extender- und Win16-Anwendungen, die auf den HASP-Gerätetreiber zugreifen.
-120	DOS-Speicher kann nicht allokiert werden. Bei DOS-Extender und Windows-Anwendungen, die mit HASP-Keys für Einzelrechner geschützt wurden. Versuchen Sie, DOS-Speicher freizugeben.
-121	Fehler beim Freigeben von DOS-Speicher. Bei DOS-Extender und Windows-Anwendungen, die mit HASP-Keys für Einzelrechner geschützt wurden.
-157	NH-Puffer zu klein. Wenn der Puffer während des Ver- oder Entschlüsselns von Daten kleiner 8 Bytes ist, wird die Fehlermeldung zurückgegeben. Dies gilt nur für Win32- und Win64-Anwendungen. Bezieht sich auf die Dienste 88 und 89.
-999	Ungültiger Dienst.

Tabelle 2 – HASP Fehlercodes

9 Abbildungsverzeichnis

10 Tabellen

11 SICHWORTVERZEICHNIS

A

B

C

D

E

F

H

I

K

L

M

P

R

S

V