Benutzerhandbuch

AutoSigner DataCenter-Edition

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 DOKOMENTENVERLAUF

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	13.07.17	Anpassungen CI	OM

2 EINLEITUNG

2.1 INHALT

Das vorliegende Handbuch macht Sie mit den Komponenten der Signaturanwendung AutoSigner DCE bekannt. Es beschreibt die Installation, die Ersteinrichtung und die Verwendung der gelieferten Software. In den folgenden Abschnitten finden Sie Informationen zur Durchführung folgender kryptographischer Vorgänge:

- Erstellen elektronischer Signaturen

Dieses Handbuch wendet sich an Anwender und Administratoren, die die Signaturanwendungskomponente AutoSigner DCE installieren und verwenden wollen. Es enthält **keine** Beschreibung, wie die Unterstützung einer spezifischen Smartcard unter dem verwendeten Betriebssystem sichergestellt werden kann.

2.2 AUFBAU DES HANDBUCHES

Das Handbuch gliedert sich in sechs Kapitel mit den folgenden Schwerpunkten:

- Kapitel 2 beinhaltet diese Einleitung.
- Kapitel 3 beschreibt die Anforderungen, die für den Einsatz der Software gelten.
- Kapitel 4 beschreibt die Installation und Grundkonfiguration des AutoSigner DCE.
- Kapitel 5 enthält Einsatzempfehlungen für die Software.
- Kapitel 6 enthält Beschreibungen zur Verwendung der Software.
- Kapitel 7 beschreibt die Konfigurationsmöglichkeiten.
- Kapitel 8 beschreibt die Grundlagen der elektronischen Signatur.
- Kapitel 9 enthält die Beschreibung der Logokonfiguration per XML-Datei.
- Kapitel 10 beschreibt die Protokollierung in Log-Dateien.

3 SYSTEMVORAUSSETZUNGEN

3.1 ANFORDERUNGEN AN DIE HARDWARE

- IBM-PC kompatibler Personal Computer ab Pentium 4
- mindestens 2048 MByte Arbeitsspeicher
- mindestens 80 MByte freier Festplattenspeicher
- Bildschirmauflösung mindestens 800x600 Pixel
- USB Port(s) für Kartenleser / USB2LAN für Anbindung der Kartenleser
- CD-ROM für die Installation bzw. Internet-Verbindung für den Download der Setupdateien.
- Chipkarten-Leser der Klasse II mit CT-API Unterstützung
  - Chipdrive Pinpad Pro (SPR 532x)
  - Reiner CyberJack SCT
  - Kobil Kaan Standard Plus USB
- eine persönliche Signaturkarte bzw. ein Software-Zertifikat

3.2 ANFORDERUNGEN AN DIE SOFTWARE

- eines der unterstützten Betriebssysteme

  - Microsoft Windows Server 2008 / 2008 R2
  - Microsoft Windows Server 2012 / 2012 R2
  - Microsoft Windows Vista SP1 bis EOL (11.04.2017)
  - Microsoft Windows 7
  - Microsoft Windows 8.1
  - Microsoft Windows 10
  - Linux verschiedene Derivate möglich empfolen wird zurzeit Debian ab Version 7.x
- Evtl. ein installierter kryptographischer Serviceprovider

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

3.3 UNTERSTÜTZTE TRUSTCENTER

Der Einsatz von Karten der folgenden Trustcenter wurde getestet und freigegeben:

- D-Trust (www.d-trust.net)
- Deutsches Gesundheitsnetz (www.dng.de)
- Bundesnotarkammer (www.bnotk.de)
- T-Systems (www.telesec.de)
- DATEV (www.datev.de)

Weitere Details zu den unterstützten Kartenleser und Signaturkarten entnehmen Sie bitte der aktuellen Herstellererklärung.

4 INSTALLATION DER SIGNATURANWENDUNGSKOMPONENTE

Rufen sie den Setupassistenten auf, der Sie im Folgenden durch die notwendigen Installationsschritte begleitet.

Vor der Installation kann auch der Installationsort angegeben werden (Abbildung 1).

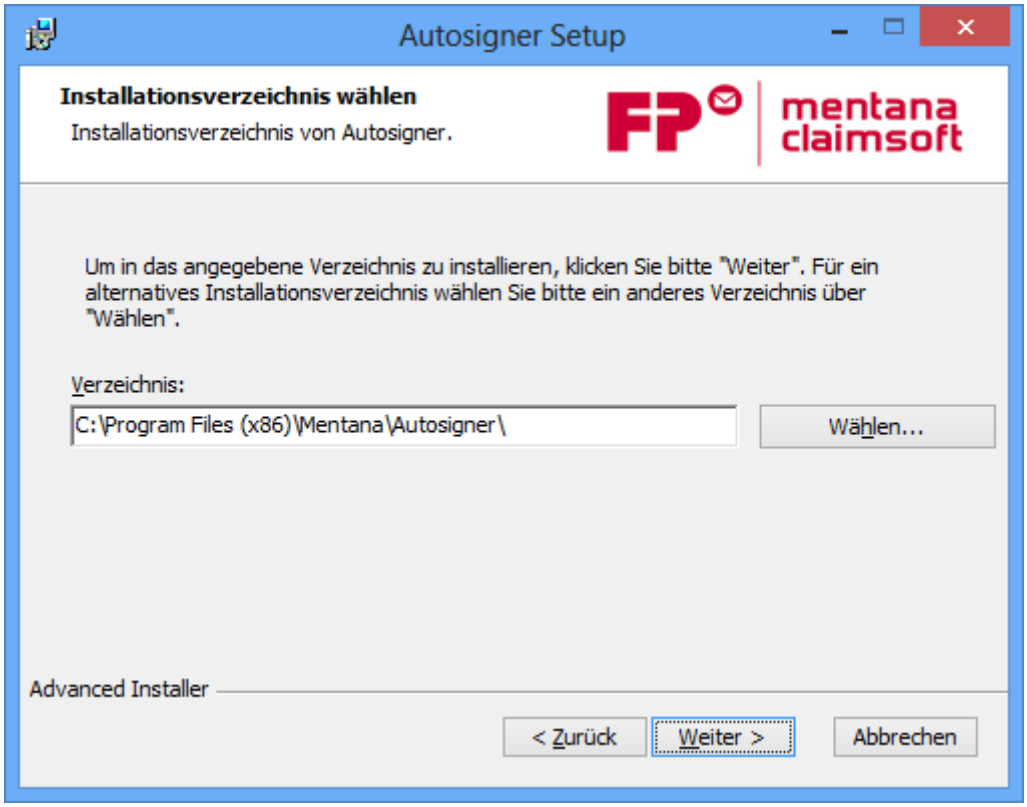

Abbildung 1 – Wahl des Installationsortes

Nach der Installation steht ein entsprechender Systemdienst zur Verfügung, der unter dem Namen „Mentana AutoSigner DCE“ in der Windows-Dienstverwaltung (services.msc) gesteuert werden kann.

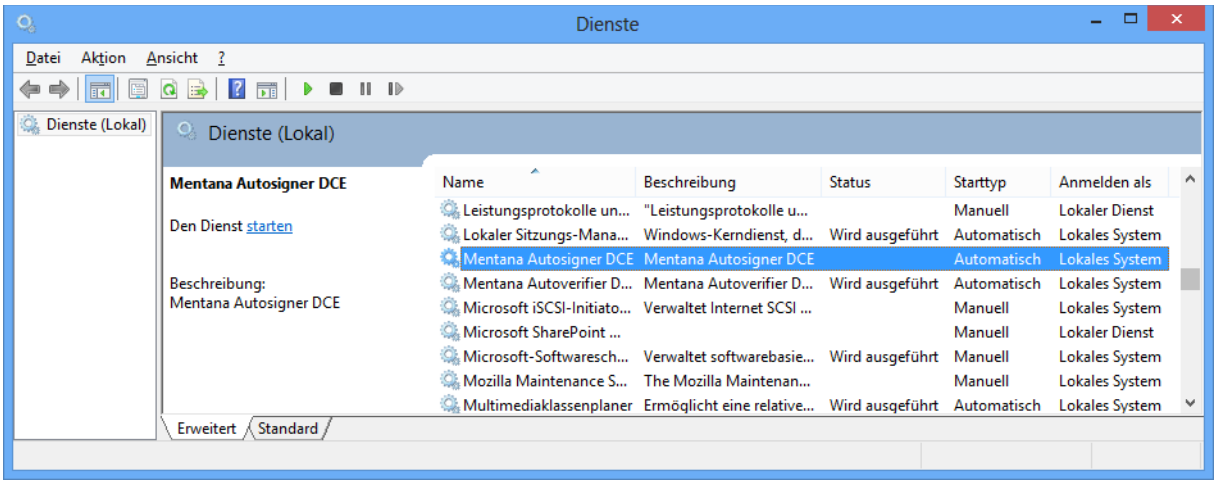

Abbildung 2: AutoSigner DCE in der Windows-Dienstverwaltung

4.1 INSTALLATION DER ALGORITHMENUNTERSTÜTZUNG

Im Anschluss an die Installation des AutoSigner DCE sollte auch die Unterstützung für weitere Signaturalgorithmen installiert werden. Ein entsprechendes Paket („Algo-Support.exe“) liegt den Installationsdateien bei. Ohne die Installation der Algorithmenunterstützung ist eine Verwendung des SHA-256-Algorithmus unter Windows XP bzw. Windows Server 2003 nicht möglich.

4.2 ERSTKONFIGURATION DER AUTOSIGNER DCE INSTANZ

Vor der ersten Verwendung sollten einige Grundeinstellungen vorgenommen werden. Genauere Konfigurationshinweise entnehmen Sie bitte dem Kapitel „Konfiguration“.

Nach der erfolgreichen Installation sollte der neue Dienst einmal gestartet und wieder gestoppt werden, um eine Konfigurationsdatei zu erstellen. Im Unterordner „svcconf“ des Installationsverzeichnisses wird dadurch eine Konfigurationsdatei (config3.xml) angelegt, die noch angepasst werden muss.

4.3 ANPASSEN DER ARBEITSVERZEICHNISSE

Im Abschnitt **<filestoreengine>** ist die Konfiguration der Arbeitsverzeichnisse hinterlegt. Hier können die zu verwendenden Arbeitsverzeichnisse konfiguriert werden. Bitte achten Sie darauf, dass die hier angegebenen Verzeichnisse im Dateisystem existieren.

```
<filestoreengine>
    <folders>
        <in>C:\Programme (x86)\Mentana\Autosigner DCE\in</in>
        <out>C:\Programme (x86)\Mentana\Autosigner DCE\out</out>
        <backup>C:\Programme (x86)\Mentana\Autosigner DCE\backup</backup>
        <error>C:\Programme (x86)\Mentana\Autosigner DCE\error</error>
    </folders>
</filestoreengine>
```

Abbildung 3: Konfiguration der Arbeitsverzeichnisse

- in: Ordner der auf zu signierende Dateien überprüft wird
- out: Ordner der die signierten Dokumente enthält
- backup: Ordner in dem Backups der Dokumente abgelegt werden
- error: Ordner für Dokumente, die nicht erfolgreich signiert wurden

Auch **UNC-Pfade** können hier verwendet werden. Bitte beachten Sie hierbei aber unbedingt, dass die Pfade eventuell nicht für das Systemkonto erreichbar sind, in dessen Kontext der Dienst standardmäßig läuft.

4.3.1 ANPASSEN DES SIGNATURALGORITHMUS

Bitte überprüfen Sie auf jeden Fall, ob der eingetragene Signaturalgorithmus ihren Wünschen entspricht und ob die konfigurierten Verzeichnisse vorhanden sind oder eventuell auch noch angepasst werden müssen.

Der verwendete Hash-Algorithmus wird unter dem Punkt <digestalgo> konfiguriert. Hier sind folgende Werte möglich:

- SHA1 = Verwendung des SHA-160 Algorithmus
- SHA-256 = Verwendung des SHA-256 Algorithmus (empfohlen)
- RIPEMD-160 = Verwendung des Ripemd-160 Algorithmus

4.3.2 ANPASSEN DER SMARTCARD-STEUERUNG

Der AutoSigner DCE wird mit einer eingebauten Kartenlesersteuerung ausgeliefert. Diese ermöglicht es unabhängig von einem CSP zu arbeiten. Solle der Windows-Zertifikatsspeicher verwendet werden, ist dies unter dem Punkt <cspmode> konfigurierbar. Hier können zwei Werte eingetragen werden:

- WINDOWS_CERTSTORE = Verwendung des Zertifikatsspeichers
- MENTANA_CSP = Verwendung der eingebauten Kartenlesersteuerung (empfohlen)

4.3.3 ANPASSEN DER REMOTEVERBINDUNG

```
<remoteconnector>
    <activated>true</activated>
    <!-- Der genutzte Port -->
    <port>7890</port>
    <users>
        <!-- Hier können die Nutzer verwaltet werden -->
        <user-account>
            <name>administrator</name>
            <password>changeoninstall</password>
        </user-account>
        <user-account>
            <name>otherUser</name>
            <password>changeoninstall</password>
        </user-account>
    </users>
</remoteconnector>
```

Abbildung 4: Konfigurationsabschnitt – remoteconnector

Die Konfiguration der Remoteverbindung wird im Abschnitt **<remoteconnector>** vorgenommen. Hier kann der zu verwendende Port (**<port>**) konfiguriert werden und die Nutzer verwaltet werden. Dieser Port kann dann von der AutoSigner DCE Web-Konsole verwendet werden.

Im Abschnitt **<users>** können mehrere Benutzer eingerichtet werden. Pro Nutzer gibt es einen Eintrag **<user-account>** mit jeweils einem Wert für Benutzername und Passwort (vgl. Abbildung 4).

Nach einer Standardinstallation ist der Connector über den Port 7890 erreichbar und es ist ein Nutzer „administrator“ mit dem Passwort „changeoninstall“ eingerichtet.

4.4 LIZENSIEREN DER ANWENDUNG

Die Verwendung des AutoSigner DCE setzt den Besitz eines gültigen Lizenzschlüssels voraus. Diesen erhalten Sie entweder als Bestandteil des gelieferten Softwarepaketes oder auf Anfrage von der Mentana-Claimsoft AG. Falls Sie zum Zeitpunkt der Installation keine Lizenz-Datei besitzen, kontaktieren Sie bitte info@mentana.de. Sie erhalten daraufhin entweder ihre endgültige Lizenzdatei bzw. einen Evaluationsschlüssel.

Um die Anwendung zu lizensieren, muss die Lizenzdatei (license.xml) im Konfigurationsverzeichnis (svcconf) des Dienstes abgelegt werden.

5 EINSATZEMPFEHLUNGEN

Die qualifizierte elektronische Signatur ist der händischen Unterschrift juristisch gleichgestellt. Das eingesetzte Signatursystem ist also als kritische Ressource zu betrachten und erfordert ein Mindestmaß an Sicherheitsmaßnahmen. Die durchzuführenden Maßnahmen sind insbesondere:

- Halten Sie die PIN Ihrer Signaturkarte in jedem Fall geheim.
- Verwenden Sie auf dem Signaturrechner eine Zugangskontrolle unter Verwendung sicherer Passworte.
- Überprüfen Sie Ihr Signatursystem regelmäßig auf bekannte Sicherheitslücken[1].
- Installieren Sie regelmäßig die vom Betriebssystemhersteller zur Verfügung gestellten Sicherheitsupdates[2].
- Nutzen Sie einen aktuellen Virenscanner.
- Sichern Sie Ihr Netzwerk gegen Eindringlinge durch den Einsatz einer Personal Firewall.
- Installieren Sie ein Anti-Spyware Programm[3].

6 VERWENDEN DES AUTOSIGNER DCE

Zum Steuern des AutoSigner DCE verwenden Sie bitte eine der bereitgestellten Steuerkonsolen. Diese verbinden sich mit der Instanz über die konfigurierte Remote-Schnittstelle und erlauben es so, mehrere Instanzen über das Netzwerk zu steuern und zu kontrollieren.

6.1 STARTEN UND STOPPEN EINER INSTANZ

Eine AutoSigner DCE Instanz lässt sich über die Dienstverwaltung von Windows starten und stoppen. Diese ist über den Aufruf „services.msc“ aufrufbar.

---

[1] Hierfür benötigte Programme finden Sie beispielsweise unter www.bsi.de

[2] Diese finden Sie z.B. unter www.windowsupdate.com

[3] Beispielsweise Microsoft Defender, Download unter www.microsoft.com

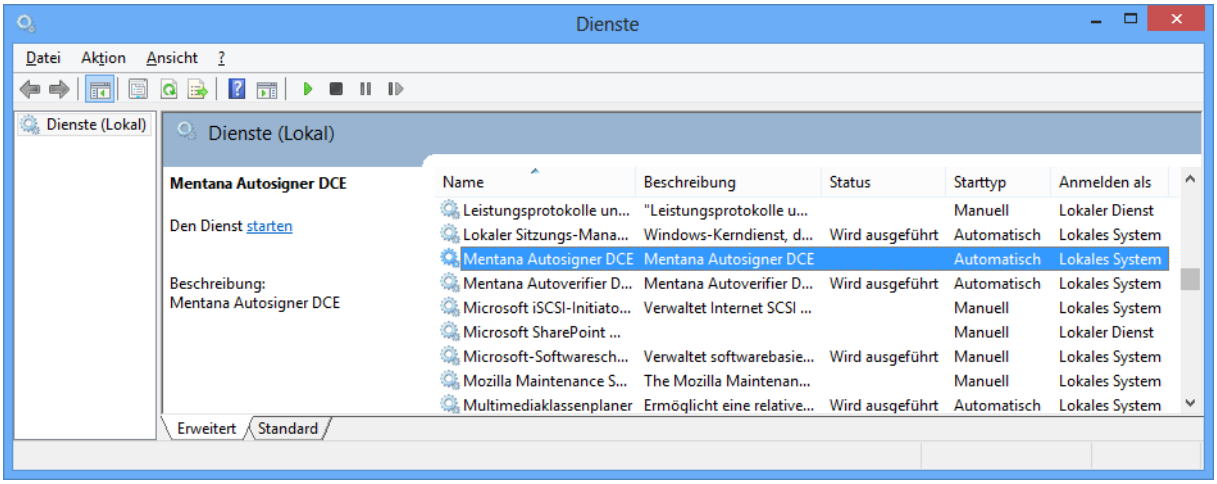

Abbildung 5: AutoSigner DCE in der Windows-Dienstverwaltung

Alternativ lässt sich die Instanz auch über den Kommandozeilenaufruf „net {start |stop} asdce“ steuern. Bitte beachten Sie, dass für das Starten und Stoppen von Windows-Diensten evtl. erhöhte Rechte benötigt werden.

Durch das Starten des Dienstes wird nicht automatisch eine Signatursession eröffnet. Dies muss über die mitgelieferte Verwaltungskonsole geschehen.

6.2 ERSTELLEN ELEKTRONISCHER SIGNATUREN

Nachdem über eine Verwaltungskonsole der Startbefehl an den AutoSigner DCE gesendet wurde, startet dieser den Signaturvorgang. Bei Verwendung eines Kartenlesers muss nach dem Aufruf die PIN am Gerät eingegeben werden.

Das konfigurierte Eingangsverzeichnis wird hierbei regelmäßig nach neuen Dokumenten durchsucht, die signiert und in den Ausgangsordner verschoben werden. Dokumente, bei denen die Signatur nicht erfolgreich war, werden im „error“-Verzeichnis abgelegt. Falls gewünscht, kann von jedem Dokument vor der Signatur ein Backup erstellt werden (vgl. Kapitel „Konfiguration“).

In Abhängigkeit vom Typ des zu unterzeichnenden Dokumentes unterstützt der AutoSigner DCE zwei verschiedene Signaturmodi.

- **Interne Signatur**: Bei diesem Verfahren wird die elektronische Signatur vollständig in das Dokument eingebettet. Der Empfänger erhält nur eine Datei, in der sowohl ursprüngliches Dokument als auch die kryptographische Signatur enthalten ist. Mehrfach signierte Dokumente bzw. mehrere, signierte Versionen innerhalb eines Dokumentes sind möglich. Diese Option steht jedoch nur für Dokumente im PDF-Format zur Verfügung.
- **Externe Signatur**: Bei diesem Verfahren wird eine weitere Datei erzeugt, in der die kryptographischen Daten im PKCS#7-Format abgelegt werden. Bei diesem Verfahren benötigt der Empfänger das Ausgangsdokument und die Signaturdatei, um die Signatur prüfen zu können, d.h. Urheber und Integrität eines empfangenen Dokumentes feststellen zu können.

7 KONFIGURATION

7.1 STARTOPTIONEN DES DIENSTES

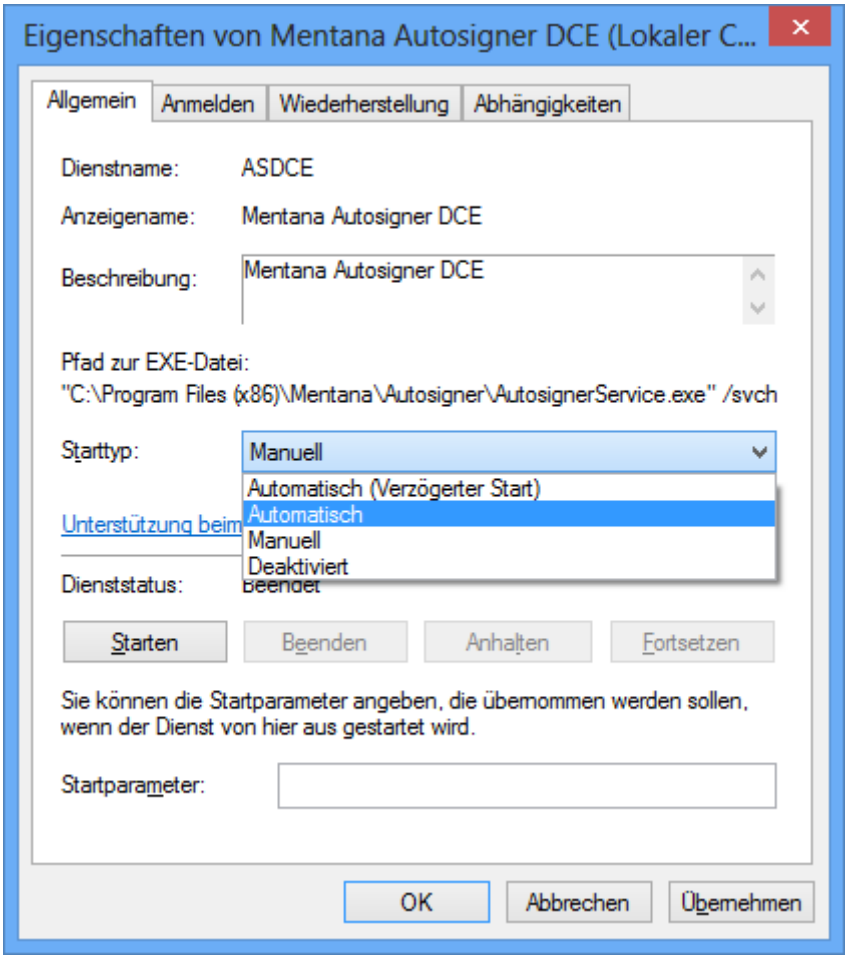

Abbildung 6: Startoptionen des Windows-Dienstes

Über die Windows-Dienstverwaltung (services.msc) lässt sich das Startverhalten beim Hochfahren des Systems steuern. Über einen Doppelklick auf den Dienstnamen („Mentana AutoSigner DCE“) kann man die entsprechenden Einstellungen ändern.

Wie in Abbildung 6 zu sehen, stehen hier 4 Optionen zur Verfügung:

- **Automatisch** Der Dienst startet automatisch, wenn Windows hochgefahren wird.
- **Automatisch (Verzögerter Start)** Der Dienst startet automatisch, wenn Windows hochgefahren wird, allerdings wird der Dienst erst verzögert gestartet
- **Manuell** Der Dienst wird nicht automatisch gestartet, sondern muss manuell aufgerufen werden.
- **Deaktiviert** Der Dienst wird gar nicht gestartet und kann auch nicht manuell gestartet werden.

7.2 KONFIGURATION DER INSTANZ

Die Einstellungen einer Instanz werden in der Datei config3.xml festgehalten, die im Konfigurationsverzeichnis des Dienstes (svcconf) liegt. Ist die Datei nicht vorhanden, starten

Sie den Dienst einmal und beenden ihn wieder. Dies wird eine Standardkonfigurationsdatei anlegen.

6.2.1 GRUNDEINSTELLUNGEN

6.2.1.1 ANPASSEN DER SMARTCARD-STEUERUNG

Der AutoSigner DCE wird mit einer eingebauten Kartenlesersteuerung ausgeliefert. Diese ermöglicht es, unabhängig von einer vorhandenen CSP zu arbeiten. Soll jedoch der Windows-Zertifikatsspeicher verwendet werden, ist dies unter dem Punkt **<cspmode>** konfigurierbar. Hier können zwei Werte eingetragen werden:

- WINDOWS_CERTSTORE = Verwendung des Zertifikatsspeichers
- MENTANA_CSP = Verwendung der eingebauten Kartenlesersteuerung

```
<configuration product="Mentana AutoSigner DCE" version="2.1">
    <core>
        ...
        <cspmode>MENTANA_CSP</cspmode>
```

Abbildung 7: Konfiguration der Smartcard-Steuerung

Soll der Windows-Zertifikatsspeicher verwendet werden, muss darauf geachtet werden, dass die zu verwendenden Zertifikate im Benutzer-Kontext, unter dem der AutoSigner DCE läuft, zur Verfügung stehen.

6.2.1.2 ANPASSEN DES SIGNATURALGORITHMUS

Bitte überprüfen Sie auf jeden Fall, ob der eingetragene Signaturalgorithmus ihren Wünschen entspricht. Wenn nicht, muss dies unbedingt angepasst werden.

Der verwendete Hash-Algorithmus wird unter dem Punkt **<digestalgo>** konfiguriert. Hier sind folgende Werte möglich:

- SHA1 = Verwendung des SHA-160 Algorithmus
- SHA-256 = Verwendung des SHA-256 Algorithmus (empfohlen)
- SHA-384 = Verwendung des SHA-384 Algorithmus
- SHA-512 = Verwendung des SHA-512 Algorithmus
- RIPEMD-160 = Verwendung des Ripemd-160 Algorithmus

6.2.1.3 KONFIGURIEREN DER REMOTEVERBINDUNG

Die Steuerung des AutoSigner DCE findet über eine eingebaute Netzwerk-Schnittstelle statt. Die verwendeten Steuerungskonsolen greifen auf diese Schnittstelle zu und authentifizieren sich mittels Benutzername und Passwort.

```
<remoteconnector>
    <activated>true</activated>
    <!-- Der genutzte Port -->
    <port>7890</port>
    <users>
        <!-- Hier können die Nutzer verwaltet werden -->
        <user-account>
            <name>administrator</name>
            <password>changeoninstall</password>
        </user-account>
        <user-account>
            <name>otherUser</name>
            <password>changeoninstall</password>
        </user-account>
    </users>
</remoteconnector>
```

Abbildung 8: Konfigurationsabschnitt – remoteconnector

Die Konfiguration der Remoteverbindung wird im Abschnitt **<remoteconnector>** vorgenommen. Hier kann der zu verwendende Port (**<port>**) konfiguriert werden und die Nutzer verwaltet werden.

Im Abschnitt **<users>** können mehrere Benutzer eingerichtet werden. Pro Nutzer gibt es einen Eintrag **<user-account>** mit jeweils einem Wert für Benutzername und Passwort (vgl. Abbildung 8).

Ein Deaktivieren der Schnittstelle (<activated>false</activated>) wird nicht empfohlen, da sonst die Instanz von außen nicht mehr steuerbar ist.

6.2.1.4 ANWENDUNGSMODI

Der AutoSigner DCE bietet verschiedene Anwendungsmodi, die je nach Lizensierung zur Verfügung stehen. Diese werden unter dem Punkt **<operationmode>** konfiguriert.

```
<configuration product="Mentana AutoSigner DCE" version="2.1">
    <core>
        <operationmode>FILESTORE</operationmode>
```

Abbildung 9: Einstellung des Operationsmodus

Die Standardversion des AutoSigner DCE stellt die Verwendung der Dateisystem-Schnittstelle zur Verfügung („FILESTORE“). Weitere mögliche Werte sind hier:

- *FILESTORE* Verwendung der Dateisystemschnittstelle
- *SOAP* Verwendung der SOAP-Schnittstelle
- *SMTP* Verwendung der SMTP-Schnittstelle

In diesem Handbuch wird nur die Verwendung der Dateisystem-Schnittstelle behandelt. Sollten Sie Informationen zu den weiteren Modulen wünschen, wenden Sie sich bitte an den Hersteller.

6.2.1.5 LOGGING

```
<configuration product="Mentana Autosigner DCE" version="2.1">
    <core>
        ...
        <logging>
            <threshold>
                <eventview>INFORMATION</eventview>
                <email>ERROR</email>
            </threshold>
            <emailsettings>
                <recipient/>
                <replyto/>
                <server/>
                <user/>
                <passwd/>
            </emailsettings>
            <logger>
                <type>ROLLINGFILE</type>
                <location>C:\Programme (x86)\Mentana\Autosigner DCE\logging</location>
            </logger>
        </logging>
```

Abbildung 10: Konfiguration des Loggingvorgangs

Im Abschnitt **<logging>** wird die Konfiguration für das Logging vorgenommen. Logausgaben werden im Event Log abgelegt, das von der Konsole ausgelesen werden kann. Ergänzend können Logdateien im Dateisystem erstellt werden und eine Mailbenachrichtigung eingerichtet werden.

Im Bereich **<threshold>** werden für das Event-Log und die Mailbenachrichtigung die zu protokollierenden Detailgrade eingestellt. Mögliche Werte sind hier:

- *INFORMATION* Alle Informationen
- *CRITICAL* Kritische Informationen
- *ERROR* Fehler
- *FATAL* Ausnahmefehler

Für das Versenden von Mailbenachrichtigungen müssen der Empfänger, die Antwortadresse und die Zugangsdaten zum Mailserver bzw. Mailprovider eingetragen werden.

Die Textdateiprotokollierung wird im Abschnitt **<logger>** konfiguriert. Wichtig ist hier nur die Angabe eines Ordners, in den die Log-Dateien abgelegt werden (**<location>**).

6.2.1.6 SIGNATUREIGENSCHAFTEN

Im Konfigurationsabschnitt **<signature>** werden die Signatureigenschaften definiert.

```
<configuration product="Mentana Autosigner DCE" version="2.1">
    <core>
        ...
        <signature>
            <checksignatures>true</checksignatures>
            <mapping>
                <pdf>PDF_SIG</pdf>
                <image>CONVERT_IMAGE</image>
                <xml>SMIME_DETACHED</xml>
                <binary>SMIME_DETACHED</binary>
            </mapping>
            <properties>
                <pdfsignature>
                    <reason/>
                    <location/>
                    <contact/>
                    <tsa/>
                    <appearances>
                        <signaturefield>
                            <name>Signiert mit AutoSigner</name>
                            <definition> C:\Programme (x86)\Mentana\Autosigner DCE\aslogo.xml</definition>
                            <anchor>ABS_BOTTOM_LEFT</anchor>
                            <coordinates>
                                <x-origin>50</x-origin>
                                <y-origin>50</y-origin>
                            </coordinates>
                            <default>true</default>
                        </signaturefield>
                    </appearances>
                </pdfsignature>
            </properties>
        </signature>
```

Abbildung 11: Konfigurationsabschnitt – Signatureigenschaften

<checksignatures> steuert die Überprüfung der Signaturintegrität nach dem Signaturvorgang. Die empfohlene Einstellung ist „true“. Wird hier „false“ eingetragen, wird die Integrität der Signatur nach erfolgter Signatur nicht geprüft.

Der Abschnitt **<mapping>** steuert die Verarbeitung verschiedener Dateitypen. Es werden folgende Dateitypen unterschieden:

- *pdf* PDF-Dokumente
- *image* Bilddateien (jpeg und gif)
- *xml* XML-Dokumente
- *binary* alle weiteren Dateien

Für alle Dokumente können folgende Einstellungen gewählt werden:

- *SMIME_DETACHED* S/MIME kompatible, externe Signatur
- *SMIME_EMBEDDED* eingebettete PKCS#7-Signatur
- *IGNORED* Dokumententyp wird nicht signiert.

PDF-Dokumente können darüber hinaus mit einer unsichtbaren (Wert: *PDF_SIG*) oder sichtbaren (Wert: *PDF_VISIBLE_SIG*) Unterschrift versehen werden.

Bilddateien können optional in eine PDF-Datei konvertiert werden, bevor sie signiert werden. Dies kann man über dem Eintrag *CONVERT_IMAGE* beim Tag Image einstellen.

Im Abschnitt **<pdfsignature>** können Eigenschaften der PDF-Unterschriften näher definiert werden:

Neben einem Grund (**<reason>**), einem Ort (**<location>**) und einem Ansprechpartner (**<contact>**) kann hier auch die URL (Adresse) eines RFC3161-kompatiblen Zeitstempelanbieters (**<tsa>**) angegeben werden. Ist hier eine entsprechende URL konfiguriert, werden bei allen PDF-Signaturen ein Zeitstempel abgerufen und eingebettet. Achtung: Dabei können Kosten entstehen!

Im Bereich **<signaturefield>** kann die sichtbare Unterschrift genauer konfiguriert werden.

Das Tag **<name>** stellt hier den Platz für eine Bezeichnung bereit.

Das Tag **<anchor>** bestimmt die Position des Signaturfelds. Mögliche Einträge sind hier:

- REL_BOTTOM_LEFT — Relativ zu links unten (Angabe in Prozent)
- ABS_BOTTOM_LEFT — unten links (Angabe in Pixeln)
- ABS_TOP_LEFT — oben links (Angabe in Pixeln)
- ABS_BOTTOM_RIGHT — unten rechts (Angabe in Pixeln)
- ABS_TOP_RIGHT — oben rechts (Angabe in Pixeln)

Abhängig von der in **<anchor>** bestimmten Position kann unter **<coordinates>** die Position des Feldes genau bestimmt werden. Die Angaben für x- und y-Koordinaten sind entsprechend der oben gewählten Angabe entweder relativ oder absolut zu verstehen.

Das Tag **<definition>** verweist auf eine XML-Datei, die die genaue Beschreibung des Signaturfeldes enthält. Eine Erläuterung hierfür finden Sie im Kapitel 9 an diese Anleitung.

6.2.1.7 SESSION

Die im Abschnitt **<session>** hinterlegten Daten sind für zukünftige Versionen eingeplant und sollten momentan noch nicht verändert werden.

6.2.1.8 REVIEW

Die im Abschnitt **<review>** hinterlegten Daten sind für zukünftige Versionen eingeplant und sollten momentan noch nicht verändert werden.

6.2.2 DIE DATEISYSTEMSCHNITTSTELLE

6.2.2.1 ANPASSEN DER ARBEITSVERZEICHNISSE

Im Abschnitt **<filestoreengine>** können die zu verwendenden Arbeitsverzeichnisse konfiguriert werden. Bitte achten Sie darauf, dass die hier angegebenen Verzeichnisse im Dateisystem tatsächlich existieren.

```
<filestoreengine>
    <folders>
        <in>C:\Programme (x86)\Mentana\Autosigner DCE\in</in>
        <out>C:\Programme (x86)\Mentana\Autosigner DCE\out</out>
        <backup>C:\Programme (x86)\Mentana\Autosigner DCE\backup</backup>
        <error>C:\Programme (x86)\Mentana\Autosigner DCE\error</error>
    </folders>
</filestoreengine>
```

Abbildung 12: Konfiguration der Arbeitsverzeichnisse

- *in:* Ordner, der auf zu signierende Dateien überprüft wird
- *out*: Ordner, der die signierten Dokumente enthält
- *backup*: Ordner, in dem Backups der Dokumente abgelegt werden
- *error*: Ordner für Dokumente, die nicht erfolgreich signiert wurden

Auch **UNC-Pfade** können hier verwendet werden. Bitte beachten Sie hierbei aber unbedingt, dass die Pfade eventuell nicht für das Systemkonto erreichbar sind, in dessen Kontext der Dienst standardmäßig läuft.

6.2.2.2 DATEIHANDLING

Im Abschnitt **<behaviour>** können weitergehende Einstellungen bei der Verwendung der Dateisystemschnittstelle konfiguriert werden.

```
<configuration product="Mentana Autosigner DCE" version="2.1">
    <core>
        ...
        <filestoreengine>
            ...
            <behaviour>
                <createbackup>true</createbackup>
                <scansubfolders>false</scansubfolders>
            </behaviour>
```

Abbildung 13: Konfiguration des Dateihandlings

Das Tag **<createbackups>** steuert, ob in dem konfigurierten Backupverzeichnis Sicherheitskopien der zu signierenden Dokumente erstellt werden sollen. Erlaubte Werte sind „true“ und „false“.

Das Tag **<scansubfolders>** ermöglicht bei Aktivierung ein rekursives Abarbeiten des Verzeichnisinhalts. Ist diese Option aktiviert (Wert: „true“), werden auch Unterverzeichnisse des Eingangsordners durchsucht und die Ordnerstruktur im Ausgangsverzeichnis auch entsprechend erzeugt. Ist diese Option deaktiviert (Wert: „false“), wird nur der eigentliche Eingangsordner nach zu signierenden Dokumenten durchsucht. Unterverzeichnisse werden nicht verarbeitet.

6.2.2.3 DATEIERWEITERUNGEN

```
<configuration product="Mentana Autosigner DCE" version="2.1">
    <core>
        ...
        <filestoreengine>
            ...
            <extensions>
                <smime-detached>p7s</smime-detached>
                <smime-embedded>p7m</smime-embedded>
            </extensions>
```

Abbildung 14: Konfiguration der zu verwendenden Dateierweiterungen

Im Abschnitt **<extensions>** können die Dateierweiterungen für PKCS#7-Signaturen konfiguriert werden.

<smime-detached> konfiguriert die Dateierweiterung bei externen PKCS#7 Dateien.

<smime-embedded> konfiguriert die Dateierweiterung bei integrierten PKCS#7 Dateien.

Es wird empfohlen, die voreingestellten Erweiterungen beizubehalten, da diese sich an gängigen Standards orientieren.

6.2.2.4 METADATEN

Der Abschnitt **<metafiles>** wird momentan noch nicht ausgewertet.

6.2.3 KARTENLESERANBINDUNG

```
<configuration product="Mentana Autosigner DCE" version="2.1">
    <core>
        ...
        <smartcardsupport>
            <reader>
                <id>2</id>
                <name>KOBIL Systems KAAN Advanced 1</name>
                <slot>0</slot>
                <cert>0</cert>
            </reader>
        </smartcardsupport>
```

Abbildung 15: Konfiguration des Kartenlesers

Wird das interne Kartenlesermodul verwendet, muss noch die Kartenleseranbindung konfiguriert werden. Für den zu benutzenden Kartenleser werden eine Id und ein Name benötigt.

Beim ersten Start legt der AutoSigner DCE eine Datei mit dem Namen „readers.xml“ an, in der die angeschlossenen Kartenleser aufgelistet werden (vgl. Abbildung 16). Aus dieser Datei können die gewünschte Id und der gewünschte Name in die Tags **<id>** und **<name>** übernommen werden. Die Tags **<Slot>** und **<Cert>**“ werden momentan nicht ausgewertet.

```
<?xml version="1.0" encoding="ISO-8859-1" standalone="yes"?>
<readers>
    <reader>
        <id>0</id>
        <alias>FT SCR2000A 0</alias>
        <name>FT SCR2000A 0</name>
    </reader>
    <reader>
        <id>1</id>
        <alias>FT SCR2000A 1</alias>
        <name>FT SCR2000A 1</name>
    </reader>
    <reader>
        <id>2</id>
        <alias>KOBIL Systems KAAN Advanced 1</alias>
        <name>KOBIL Systems KAAN Advanced 1</name>
    </reader>
</readers>
```

Abbildung 16: Inhalt der Datei readers.xml

8 ELEKTRONISCHE SIGNATUREN IM ÜBERBLICK

Der vorliegende Abschnitt erklärt die Begriffe und die Prinzipien der digitalen Signatur. Er wird Sie mit dem notwendigen technischen und juristischen Hintergrund der Signaturanwendungskomponente AutoSigner DCE vertraut machen.

8.1 WARUM ELEKTRONISCHE SIGNATUREN BENÖTIGT WERDEN

Elektronische Medien haben in den letzten Jahren erheblich an Bedeutung gewonnen und durchdringen inzwischen weite Bereiche des Geschäfts- und des Privatlebens. Der dabei stattfindende Datenaustausch über Netzwerke erhält zentrale Bedeutung. In diesem Szenario kommunizieren Sie regelmäßig mit Personen, die Sie nicht persönlich kennen. Eine Sicherheit, dass Ihr Kommunikationspartner diejenige Person ist, für die er sich ausgibt, existiert nicht. Es ist ebenfalls zweifelhaft, ob die übermittelten Daten in derselben Form bei Ihnen eintreffen, in der sie vom Kommunikationspartner versendet wurden. Das feh-lende Vertrauen in die Authentizität und die Integrität der übertragenen Daten verhindert jegliches rechtverbindliches elektronisches Handeln. Die Lösung dieser Probleme wird durch die Verwendung der elektronischen Signatur ermöglicht. Sie

ermöglicht es dem Empfänger zweifelsfrei festzustellen, wer der Absender einer elektronischen Botschaft ist und ob die Daten während der Übertragung kompromittiert wurden. Die digitale Signatur sichert somit zwei Eckpfeiler des verbindlichen elektronischen Handelns ab:

- Der Absender einer Nachricht ist rechtskräftig und eindeutig feststellbar.
- Die Korrektheit des Inhalts der Nachricht kann bewiesen werden.

8.2 BEGRIFFSKLÄRUNG

Ähnlich wie eine von Hand geleistete Unterschrift ein unterschriebenes Dokument in Beziehung zum Unterzeichner setzt, bietet die elektronische Signatur die Möglichkeit, elektronische Dokumente eindeutig einem Signator (Unterzeichner) zuzuordnen. Der Einsatz und die Qualitätsanforderungen an die elektronische Signatur werden im Gesetz über die Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften (SigG) beschrieben. Der Gesetzestext beschreibt die Signatur als:

> *Eine digitale Signatur im Sinne dieses Gesetzes ist ein mit einem privaten Signatur-schlüssel erzeugtes Siegel zu digitalen Daten, das mit Hilfe eines zugehörigen öffentlichen Schlüssels, der mit einem Signaturschlüssel-Zertifikat einer Zertifizierungsstelle oder der Behörde nach § 3 versehen ist, den Inhaber des Signatur-schlüssels und die Unverfälschtheit der Daten erkennen lässt.* ***Signaturgesetz §2 Abs. 1***

Der Gesetzgeber unterscheidet bei der Anwendung elektronischer Signaturen vier Signaturklassen:

- **Einfache Signatur**: Die einfache Signatur erlaubt keinerlei Rückschlüsse auf den Urheber und die Integrität einer Nachricht. Sie verwendet weder kryptographische Methoden noch eine Public Key Infrastruktur (PKI), die eine Zuordnung einer Signatur zu einer natürlichen Person erlaubt. Typische Beispiele sind:
  - eingescannte Unterschriften
  - E-Mail-Signatur mit Kontaktdaten
- **Fortgeschrittene Signatur**: Die fortgeschrittene Signatur ist eine kryptographisch erzeugte Unterschrift, die die Identifizierung eines Inhabers bzw. einer E-Mail-Adresse ermöglicht. Die Identität des Schlüssel-Inhabers wird innerhalb einer Public Key Infrastruktur durch Zertifikate bzw. durch Hinterlegung des öffentlichen Schlüssels auf Schlüsselserver gewährleistet. Veränderungen an den übertragenen Daten sind durch die verwendeten kryptographischen Verfahren sicher erkennbar. Der zum Signieren benötigte private Schlüssel wird vom Inhaber selbst erzeugt und befindet sich auf einem auslesbaren Medium. Typische Beispiele sind:
  - Firmen- oder Behördeninterne PKI-Strukturen
  - Self-signed Zertifikate in Adobe Produkten
  - PGP-Signaturen
- **Qualifizierte Signatur**: Qualifizierte elektronische Signaturen sind Signaturen, bei denen eine eindeutige Zuordnung der Unterschrift zu einer natürlichen Person möglich ist. Diese Zuordnung findet unter Verwendung eines Zertifikates statt, dessen Integrität und Gültigkeitszeitraum automatisiert gegenüber einer öffentlichen PKI-Infrastruktur überprüft werden kann. Das Zertifikat enthält den

öffentlichen Schlüssel des Unterzeichners und wurde durch einen Zertifizierungsdienstanbieter (Trustcenter) ausgestellt. Im Gegensatz zur fortgeschrittenen Signatur wird zur Signaturerstellung benötigte Schlüsselpaar nicht auf dem Rechner des Versenders generiert, sondern direkt auf der Signaturkarte erzeugt. Der private Schlüssel ist hier-bei nicht exportierbar, eine Weitergabe an andere Personen ist somit ausgeschlossen.

- **Qualifizierte Signatur mit Anbieterakkreditierung**: Die qualifizierte Signatur mit Anbieterakkreditierung ist technisch mit der qualifizierten Signatur identisch. Der Abgrenzung erfolgt über das ausstellende Trustcenter. Akkreditierte Trustcenter verwenden ein Stammzertifikat, welches von der Bundesnetzagentur (BNetzA) gegengezeichnet wurde. Im Unterschied zur qualifizierten Signatur wird die Verifizier-barkeit der Zertifikate nicht für nur fünf sondern für mindestens 30 Jahre zugesichert.

8.3 TECHNISCHE GRUNDLAGEN

Die elektronische Signatur basiert auf asymmetrischer Kryptographie. Dabei wird ein zusammenhängendes Schlüsselpaar generiert, welches zur eigentlichen Datenverschlüsselung eingesetzt wird. Das Schlüsselpaar umfasst folgende Schlüssel:

- **Private key**: Der private Schlüssel wird zur Verschlüsselung von Daten verwendet. Er ist geheim und darf sich nur im Besitz des Unterzeichners befinden.
- **Public key**: Der öffentliche Schlüssel dient zur Entschlüsselung der Daten. Er kann nur diejenigen Daten entschlüsseln, die mit dem zugehörigen privaten Schlüssel verschlüsselt wurden. Im Gegensatz zu diesem ist er öffentlich und wird in Schlüsselverzeichnissen hinterlegt.

Die Verwendung asymmetrischer Verschlüsselung behebt zwei grundsätzliche Probleme der Kryptographie:

- Minimierung des Geheimnisses: Da keine gemeinsamen Schlüssel verwendet wer-den, muss jeder Schlüsselinhaber nur auf die Geheimhaltung seines privaten Schlüssels achten. Bei der qualifizierten elektronischen Signatur wird dieser Punkt durch die verwendete Technik sichergestellt.
- Schlüsselverteilungsproblem: Es werden keine abhörsicheren Kanäle zur Verteilung des gemeinsamen Schlüssels benötigt. Vielmehr kann der öffentliche Schlüssel einzig zur Entschlüsselung des Chiffrats genutzt werden.

Durch den Einsatz zertifikatsbasierter Systemen erhält jeder Schlüsselinhaber ein digitales Zertifikat, welches seine Identität beschreibt und die öffentlichen Schlüssel enthält. Jedes Zertifikat wird von einer ausgebenden Stelle beglaubigt, die ihrerseits wieder von höheren Stellen beglaubigt sein kann. Das entstehende Vertrauenssystem, die so genannte Zertifikatskette ist streng hierarchisch. Den intrinsisch vertrauenswürdigen Anfang dieser Kette bildet das Wurzelzertifikat (Root Certificate). Diese Rolle kann bei der qualifizierten Signatur nur ein staatlich zugelassenes Trustcenter einnehmen.

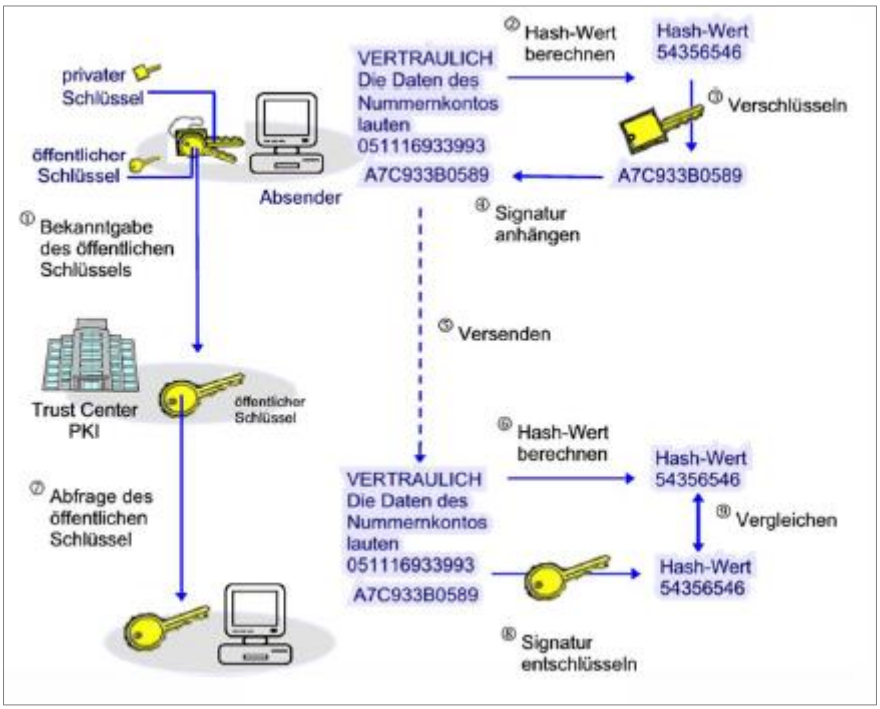

Abbildung 17: Technische Grundlagen

9 ANHANG – LOGOKONFIGURATION PER XML

Im Folgenden wird die Konfiguration einer sichtbaren Signatur beschrieben. Die Beschreibung der Logokonfiguration erfolgt über eine XML Konfigurationsdatei.

9.1 EINLEITUNG

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.

9.2 AUFBAU DER KONFIGURATIONSDATEI

Ein Beispiel der Konfigurationsdatei ist in Abbildung 25 zu sehen.

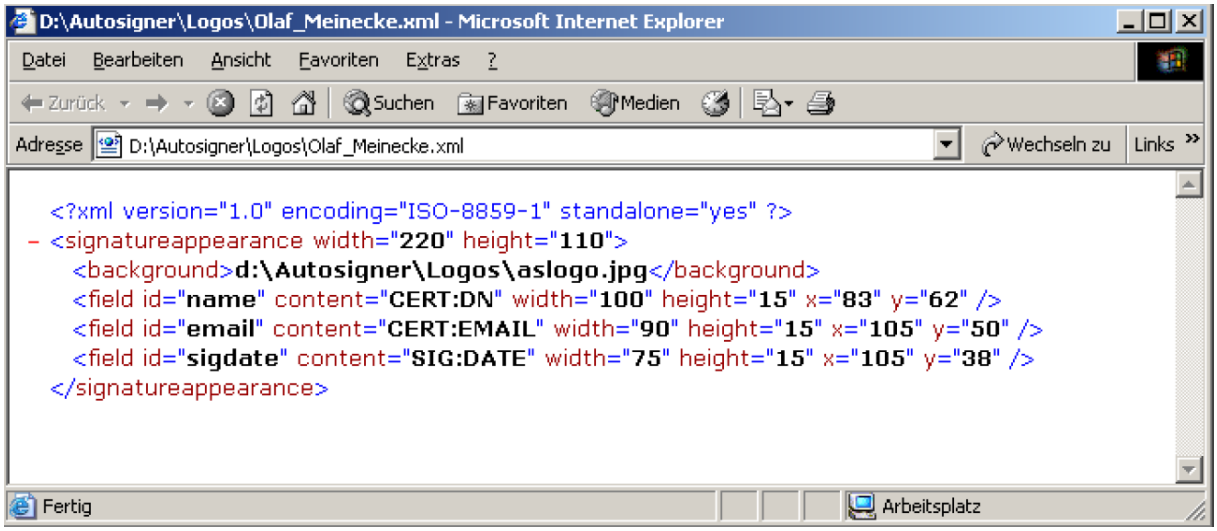

Abbildung 18: XML-Datei

Die Elemente:

<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 id>
Bestimmt die zusätzlichen Informationen, die im Signaturfeld angezeigt werden sollen. Die Eigenschaft **field id** legt einen eindeutigen Namen für ein Feld 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.

Eine graphische Darstellung der Logokonfiguration ist nachstehender Abbildung 26 zu entnehmen.

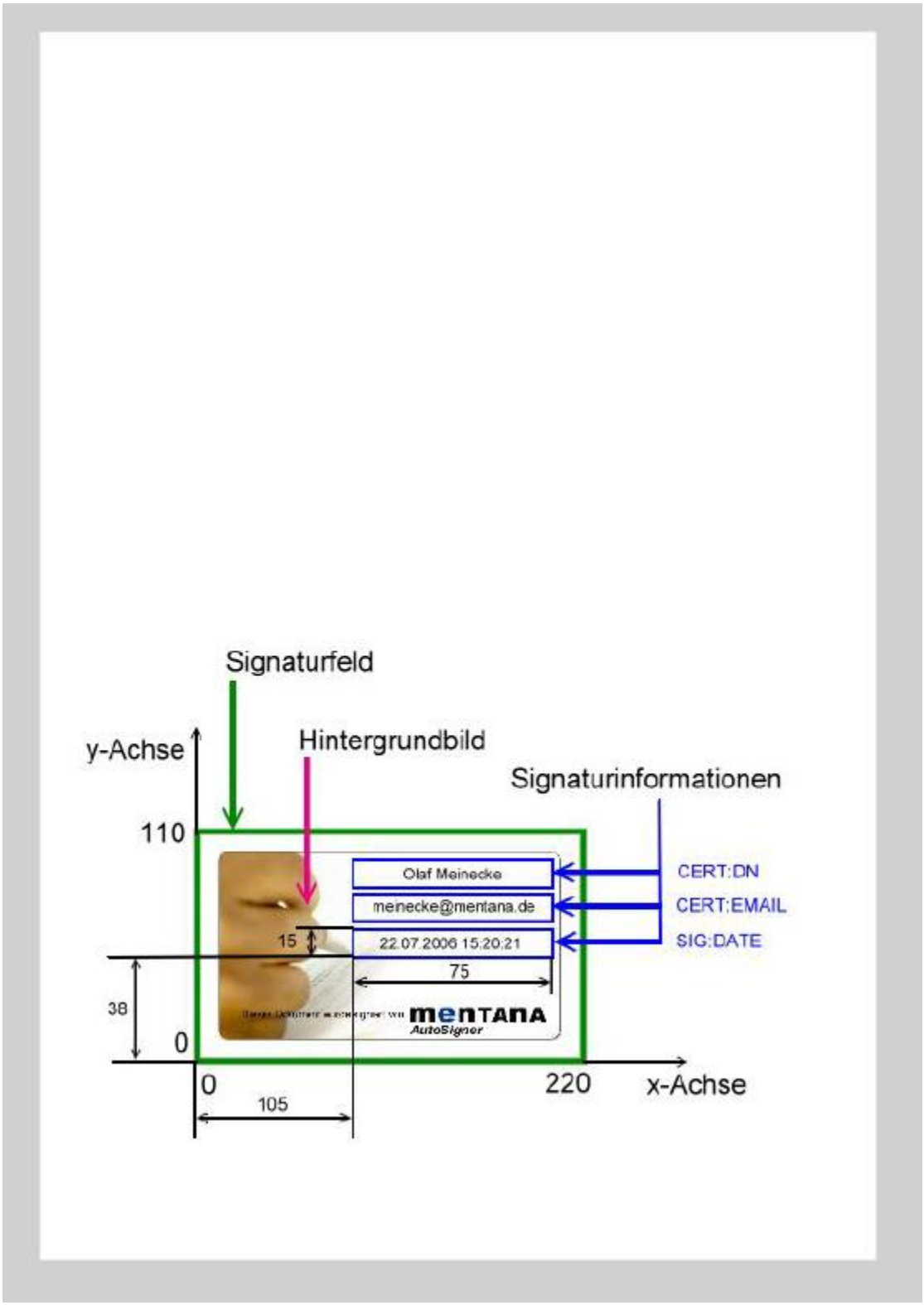

Abbildung 19: Positionierung

10 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 10.2.3).
- Info über den Start eines Signaturvorgangs.
- Welche Datei wurde signiert?
- Das Signieren einer Datei war erfolgreich oder ist fehlgeschlagen. → Ausgabe eines Fehlercodes (siehe 10.2.2).
- Abbruch des Signaturvorgangs (HASP-Key Abfrage: HASP-Key wurde z.B. während Betrieb entfernt). → Ausgabe eines Fehlercodes (siehe 10.2.3).
- 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)

10.1 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

10.2 FEHLERCODES

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

10.2.1 ALLGEMEINE FEHLER

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

10.2.2 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.

10.2.3 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

11 Abbildungsverzeichnis

12 Tabellen