Benutzerhandbuch

OfficeSigner

Version 2.2

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

INHALT

1 Einleitung 5
1.1 Inhalt 5
1.2 Aufbau des Handbuches 5
1.3 Benutzte Schriftarten/ Markierungen 5
2 Systemvoraussetzungen 6
2.1 Unterstützte Signaturerstellungseinheiten (SSEE)/ Smart-Cards 6
2.2 Unterstützte Kartenlesegeräte 10
2.3 Unterstützte Betriebssysteme 11
2.4 Einsatz nicht bestätigter Produkte 11
3 Installation 12
3.1 Installation der Anwendung 12
3.1.1 Startfenster 12
3.1.2 Lizenzbedingungen 13
3.1.3 Installationsumfang und Zielverzeichnis auswählen 13
3.1.4 Installationsverlauf 16
3.1.5 Ende der Installation 17
3.2 Lizenzierung des OfficeSigner 17
3.3 Installation Softwarezertifikat (Optional) 19
3.4 Einsatzempfehlungen 24
3.5 Überprüfen der Korrektheit der Installation 24
4 Verwenden des OfficeSigners 25
4.1 Erstellen elektronischer Signaturen 25
4.1.1 Erstellen einer eingebetteten unsichtbaren Signatur (nur PDF) 26
4.1.2 Erstellen einer eingebetteten sichtbaren Signatur (nur PDF) 32
4.1.3 Erstellen einer externen oder eingebetteten S/MIME Signatur 37
4.1.4 Erstellen von Stapelsignaturen 40
4.2 Verifizieren elektronischer Signaturen und De-Mails 42
4.2.1 Verifizieren einer eingebetteten Signatur (nur PDF) 43
4.2.2 Überprüfen eingebetteter Signaturen im Adobe Reader 48
4.2.3 Verifizieren einer externen Signatur 49
4.2.4 Verifizieren einer De-Mail 52

4.3 Erstellen qualifizierter Zeitstempel 55
4.3.1 Anmeldung beim Zeitstempeldienstleister 55
4.3.2 Anfordern eines Zeitstempels 55
4.4 Hashwert bestimmen 57
4.5 Installierte Version anzeigen 58
4.6 Lizenzierung 58
4.7 Anhang einfügen (nur PDF) 61
4.8 Steuerung über Befehlszeilen/ Parameter 63
5 Konfiguration des OfficeSigners 65
5.1 Konfiguration Allgemein 67
5.1.1 Benutzerzertifikate 68
5.1.2 Zertifikatsauswahl 69
5.1.3 Signatur 69
5.1.4 CSP 70
5.1.5 Dokumentenprüfung vor Signatur 70
5.1.6 Ausgaben 71
5.2 Konfiguration PDF-Unterschriften 71
5.3 Konfiguration S/Mime-Unterschriften 72
5.4 Konfiguration Begründungen 73
5.4.1 Hinzufügen einer Begründung 74
5.4.2 Bearbeiten einer Begründung 74
5.4.3 Löschen einer Begründung 74
5.4.4 Standard-Begründung festlegen 74
5.5 Konfiguration Orte 75
5.5.1 Hinzufügen eines Ortes 75
5.5.2 Bearbeiten eines Ortes 76
5.5.3 Löschen eines Ortes 76
5.5.4 Standard-Ort festlegen 76
5.6 Konfiguration Unterschriftspositionen 76
5.6.1 Hinzufügen einer Unterschriftsposition 77
5.6.2 Bearbeiten einer Unterschriftsposition 82
5.6.3 Löschen einer Unterschriftsposition 82

5.6.4 Standard-Unterschriftsposition festlegen 82
5.6.5 Logo mit Unterschriftsfeldern 83
5.6.6 Logokonfiguration per XML 88
5.7 Konfiguration PDF-Konvertierung 90
5.8 Konfiguration Zeitstempeldienst 90
5.9 Konfiguration Verifikation 93
5.9.1 Eigenschaften der Überprüfung 94
5.9.2 Speicherort Stylesheets Protokolle 95
5.10 Erweiterte Konfiguration 95
6 Stichwortverzeichnis 98
7 Abbildungsverzeichnis 99

1 EINLEITUNG

1.1 INHALT

Das vorliegende Handbuch macht Sie mit der Signaturanwendung OfficeSigner bekannt. Es beschreibt die Installation, die Ersteinrichtung und die Verwendung der gelieferten Software.

Dieses Handbuch wendet sich an Anwender, die die Signaturanwendungskomponente OfficeSigner installieren und verwenden wollen. Es enthält **keine** Beschreibung, wie die Unterstützung einer spezifischen Smartcard unter dem verwendeten Betriebssystem sichergestellt werden kann. Diese Informationen erhalten Sie bei den kartenausgebenden Instituten.

1.2 AUFBAU DES HANDBUCHES

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

Kapitel 2 beschreibt die Anforderungen, die für den Einsatz der Software gelten.

Kapitel 3 beschreibt die Installation der Anwendung OfficeSigner.

Kapitel 4 beschreibt den Einsatz der Software.

Kapitel 5 beschreibt erweiterte Konfigurationsoptionen für OfficeSigner.

1.3 BENUTZTE SCHRIFTARTEN/ MARKIERUNGEN

Normaler Text

Spezielle GUI-Elemente zum Anklicken

`Dateinamen, Endungen, Weblinks`

2 SYSTEMVORAUSSETZUNGEN

2.1 UNTERSTÜTZTE SIGNATURERSTELLUNGSEINHEITEN (SSEE)/ SMART-CARDS

Sichere Signaturerstellungseinheiten (SSEE)/ Smart-Cards							
Handels-bezeichnung	ZDA	Reg-Nr. ZDA	Name der SSEE in der Bestätigungs-urkunde	Bestätigung der SSEE	unterstützt wird:		
					qualifizierte Signatur	Ver-/Entschl. Authenti-sierung	Massen/Stapel-Signatur
PKS- Card (E4 NetKey 3.01)	Produkt-zentrum TeleSec Telekom AG	Z0001	SEEE TCOS 3.0 Signature Card, Version 1.0 with Philips chip P5CT072V0Q / P5CD036V0Q	TUVIT. 93119.TE.09.2006	[+][1]	[+]	[-][2]
„Multisign“	Produkt-zentrum TeleSec Telekom AG	Z0001	TCOS 3.0 Signature Card, Version 1.0 with Philips chip P5CT072V0Q / P5CD036V0Q	TUVIT. 93119.TE.09.2006	[+]	[+]	[+]
Signaturkarte der Bundesnotar kammer	Bundesnotar-kammer, Zertifizierungsstelle	Z0003	SSEE STRACOS 3.0 with Electronic Signature Application V3.0	TUVIT .93100.TE.09.2005, Nachtrag vom 08.08.2006, 20.10.2006, 07.12.2006,15.06.2007	[+]	[+]	[0][3]
Signaturkarte für Berufsträger der DATEV	DATEV eG Zertifizierungsstelle	Z0004	SSEE STRACOS 3.0 with Electronic Signature Application V3.0	TUVIT.93100.TE.09.2005, Nachtrag vom 08.08.2006, 20.10.2006,07.12.2006,15.06.2007	[+]	[+]	[0]
D-Trust-Signaturkarte Version 2.2	D-Trust GmbH	Z0017 und angezeigt § 4 Abs. 3 SigG	SSEE „Chipkarte mit Prozessor SLE66CX322P, CardOS V4.3B mit Applikation für digitale Signatur	T-Systems .02122.TE.05. 2005, Nachtrag vom 06.05.2008	[+]	[+]	[0]

[1] [+] = unterstützt
[2] [-] = nicht unterstützt
[3] [0] = Funktionalität nicht vorhanden bzw. gesperrt.

D-Trust-muticard	D-Trust GmbH	Z0017 und angezeigt § 4 Abs. 3 SigG	SSEE „Chipkarte mit Prozessor SLE66CX322P, CardOS V4.3B mit Applikation für digitale Signatur	T-Systems .02122.TE.05. 2005, Nachtrag vom 06.05.2008	[+]	[+]	[+]
SigntrustCard3.0/ Signtrust MCard100 3.0/ Signtrust MCard 3.0	Deutsche Post Com GmbH Geschäftsfeld Signtrust	Z0002	SEEE STARCOS 3.0 with Electronic Signature Application V3.0 der Giesecke & Devrient GmbH	TUVIT.93100.TE.09. 2005, Nachtrag vom 08.08.2006, 20.10.2006, 07.12.2006,15.06.2007	[+]	[+]	[+]
Signtrust Card 3.2	Deutsche Post Com GmbH Geschäftsfeld Signtrust	Z0002	SSEE STARCOS 3.2 QES Version 1.1	BSI.02102.TE.11.2008	[+]	[+]	[+]
Signtrust MCard 3.2	Deutsche Post Com GmbH Geschäftsfeld Signtrust	Z0002	SSEE STARCOS 3.2 QES Version 2.0	BSI.02114.TE.12.2008	[+]	[+]	[+]
Signtrust MCard100 3.2	Deutsche Post Com GmbH Geschäftsfeld Signtrust	Z0002	SSEE STARCOS 3.2 QES Version 2.0B	BSI.02115.TE.12.2008	[+]	[+]	[+]
TC- Trustcenter Q-Sign-Card (limited)	TC TrustCenter TrustCenter GmbH	Z0032	SEE „Chipkarte mit Prozessor SLE66CX322P, CardOS V4.3B mit Applikation für digitale Signatur	T-Systems .02122.TE.05. 2005 Nachtrag vom 06.05.2008	[+]	[+]	[0]
TC- Trustcenter Q-Sign-Card (unlimited)	TC TrustCenter TrustCenter GmbH	Z0032	SEE „Chipkarte mit Prozessor SLE66CX322P, CardOS V4.3B mit Applikation für digitale Signatur	T-Systems .02122.TE.05. 2005, Nachtrag vom 06.05.2008	[+]	[+]	[+]
Chambersign Karte der IHK D- Trust-Card (2.02c)	D-Trust GmbH	Z0017 und angezeigt § 4 Abs. 3 SigG	SEE „Chipkarte mit Prozessor SLE66CX322P, CardOS V4.3B mit Applikation für digitale Signatur	T-Systems .02122.TE.05. 2005 Nachtrag vom 06.05.2008	[+]	[+]	[0]

Sparkassen-Card oder GeldKarte	S-Trust	angezeigt § 4 Abs. 3 SigG	SEE ZKA-Signaturkarte, Version 5.02 der Gemplus-mids GmbH	TUVIT .09385.TU.09.2004	[+]	[+]	[+]
	S-Trust	Angezeigt § 4 Abs. 3 SigG	SSEE ZKA-Signaturkarte, Version 5.11	TUVIT 93138.TE.11.2006			
	S-Trust	angezeigt § 4 Abs. 3 SigG	SEE ZKA Banking Signature Card, Version 6.2b NP und 6.2f NP, Type 3 der Giesecke & Devrient GmbH	TUVIT .09395.TU.01.2005	[+]	[+]	[-]
	S-Trust	Angezeigt § 4 Abs. 3 SigG	SEE ZKA Banking Signature Card, Version 6.31 NP, Type 3 der Giesecke & Devrient GmbH	TUVIT .09397.TU.03.2005	[+]	[+]	[-]
	S-Trust	Angezeigt § 4 Abs. 3 SigG	SEE ZKA Banking Signature Card, Version 6.32 NP, Type 3 der Giesecke & Devrient GmbH	TUVIT .93125.TU.12.2005	[+]	[+]	[-]
	S-Trust	Angezeigt § 4 Abs. 3 SigG	SEE ZKA Banking Signature Card, Version 6.4 der Giesecke & Devrient GmbH	TUVIT .93123.TU.12.2006	[+]	[+]	[-]
	S-Trust	Angezeigt § 4 Abs. 3 SigG	SEE ZKA-Signaturkarte, Version 5.10 der Gemplus-mids GmbH	TUVIT .93132.TU.06.2006 20.06.2006	[+]	[+]	[-]
	S-Trust	Angezeigt § 4 Abs. 3 SigG	SEE ZKA Banking Signature Card, Version 6.6 der Giesecke & Devrient GmbH	TUVIT .93130.TU.05.2006 Nachtrag vom 28.08.2006 und vom 18.10.2006	[+]	[+]	[-]
	S-Trust	Angezeigt § 4 Abs. 3 SigG	SEE ZKA Banking Signature Card, Version 6.51 der Giesecke & Devrient GmbH	TUVIT .93129.TU.03.2006	[+]	[+]	[-]

	S-Trust	Angezeigt § 4 Abs. 3 SigG	Signaturerstellungseinheit ZKA SECCOS Sig v1.5.2 und 1.5.3 der Sagem Orga GmbH	BSI.02075.TE.08.2006 BSI.02076.TE.12.2006	[+]	[+]	[-]
	S-Trust	Angezeigt § 4 Abs. 3 SigG	ZKA-Signaturkarte, Version 5.11 M Gemplus GmbH (Gemalto)	TUVIT .93148.TU.06.2007	[+]	[+]	[+]
	S-Trust	Angezeigt § 4 Abs. 3 SigG	ZKA-Signaturkarte, Version 6	TUVIT. 93143.TE.11.2007	[+]	[+]	[-]
	S-Trust	Angezeigt § 4 Abs. 3 SigG	ZKA Banking Signature Card, Version 7.1	TUVIT. 93149.TE.09.2007	[+]	[+]	[-]
	S-Trust	Angezeigt § 4 Abs. 3 SigG	ZKA Banking Signature Card, Version 7.1.1	TUVIT. 93159.TE.09.2007	[+]	[+]	[-]
	S-Trust	Angezeigt § 4 Abs. 3 SigG	SSEE ZKA Banking Signature Card, Version 7.2.1	TUVIT. 93157.TE.06.2008	[+]	[+]	[-]
	S-Trust	Angezeigt § 4 Abs. 3 SigG	ZKA Banking Signature Card, Version 7.1.2	TUVIT. 93166.TU.06.2008	[+]	[+]	[-]
	S-Trust	Angezeigt § 4 Abs. 3 SigG	SSEE ZKA-Signaturkarte, Version 6.01	TUVIT. 93169.TU.09.2008	[+]	[+]	[-]
Signaturkarte der Deutschen Rente Bund	Deutsche Rentenversicherung Bund	Angezeigt § 4 Abs. 3 SigG	SEE „Chipkarte mit Prozessor SLE66CX322P, CardOS V4.3B mit Applikation für digitale Signatur	T-Systems .02122.TE.05. 2005, Nachtrag vom 06.05.2008	[+]	[+]	[-]
	Deutsche Rentenversicherung Bund	Angezeigt § 4 Abs. 3 SigG	SSEE "ACOS EMV-A04V1"	T-Systems. 02166.TE.07.2008 Nachtrag 1 18.12.2008 und Nachtrag 2 vom 19.05.2009	[+]	[+]	[-]

2.2 UNTERSTÜTZTE KARTENLESEGERÄTE

Handelsname	Hersteller	Name	Reg.Nr.	Schnittst.
SPR 532 usb (Chipdrive pinpad pro)	SCM Microsystems GmbH	Chipkartenleser SPR132, SPR332, SPR532, Firmware Version 4.15	TUVIT.09370.TE.03. 2003	USB, seriell
CardMan 3621	OMNIKEY	SAK Chipkartenterminal der Familie CardMan Trust CM3621, Firmware-Version 6.00	BSI.02057.TE.12 .2005	USB
CardMan 3821	OMNIKEY	SAK Chipkartenterminal der Familie CardMan Trust CM3821, Firmware-Version 6.00	BSI.02057.TE.12.2005	USB
Cherry Smartboard G83-6744	Cherry GmbH	Chipkartenterminal der Familie SmartBoard xx44 Firmware-Version 1.04	BSI.02048.TE.12. 2004	USB
Cherry SmartTerminal 2000 U	Cherry GmbH	Chipkartenterminal der Familie SmartTerminal ST-2xxx, Firmware Version 5.08	BSI.02059.TE.02. 2006	USB
Kobil KAAN Advanced	Kobil Systems GmbH	Chipkartenterminal KAAN Advanced, Hardware Version K104R3, Firmware Version 1.19	BSI.02050.TE.12.2006 vom 12.2006 und Nachtrag von T-Systems 02207.TU.04.2008	USB

(Angaben aus den veröffentlichten Bestätigungen bei der BNetzA)

2.3 UNTERSTÜTZTE BETRIEBSSYSTEME

- Microsoft Windows Server 2008 (32 und 64 Bit)
- Microsoft Terminal Services (ab Windows Server 2003)
- Microsoft Windows 7 (32 und 64 Bit)
- Microsoft Windows 8 (32 und 64 Bit)
- Microsoft Windows 8.1 (32 und 64 Bit)
- Citrix Presentation Server (ab Verson 4.0)

2.4 EINSATZ NICHT BESTÄTIGTER PRODUKTE

Die Verwendung nicht in Kapitel 1.1 und 1.2 bestätigter Produkte im Umfeld des SigG, erfordert eine herstellerseitige Einzelfallprüfung und ist nur nach ausdrücklicher schriftlicher Genehmigung durch den Hersteller zulässig.

3 INSTALLATION

3.1 INSTALLATION DER ANWENDUNG

Die Software OfficeSigner wird als Installationspaket geliefert. Dieses trägt den Namen `Setup_OS_22.msi`. Starten Sie die Einrichtung der Anwendung durch Doppelklick auf das Symbol des Installationsprogrammes (Abbildung 3-1). Sie werden aufgefordert die Lizenzbedingungen der Mentana-Claimsoft GmbH anzuerkennen, anschließend wählen Sie die zu installierenden Komponenten und ein Zielverzeichnis für die Installation der Software aus. Nach Eingabe dieser Informationen kopiert die Installationsroutine die benötigten Dateien auf ihr System und registriert Systembibliotheken.

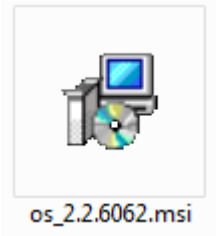

Abbildung 3-1 Setup-Icon

3.1.1 STARTFENSTER

Auf der 1. Seite des Installations-Assistenten werden Sie über die Anwendung informiert, die installiert werden soll. Klicken Sie auf Weiter, um mit der Installation fortzufahren. Zum Beenden der Installation klicken Sie auf Abbrechen.

Abbildung 3-2 Willkommen-Fenster

3.1.2 LIZENZBEDINGUNGEN

Im 2. Schritt der Installation werden Sie aufgefordert die Lizenzbedingungen zu akzeptieren. Lesen Sie sich die Lizenzbedingungen durch und klicken Sie auf Annehmen, wenn Sie mit den Lizenzbedingungen einverstanden sind. Anderenfalls klicken Sie auf Abbrechen, um die Installation zu beenden.

Abbildung 3-3 Installationsfenster mit Lizenzvereinbarung

3.1.3 INSTALLATIONSUMFANG UND ZIELVERZEICHNIS AUSWÄHLEN

In dem folgenden Schritt können Sie den Installationsumfang bestimmen.

Die Option „Standard“ installiert den OfficeSigner mit den empfohlenen Komponenten in das Programmverzeichnis des Systems (Abbildung 3-4).

Abbildung 3-4 Installationsfenster mit Komponentenauswahl

Sollen die zu installierenden Komponenten oder das Zielverzeichnis angepasst werden, wählen Sie die Option Benutzerdefiniert.

In diesen Schritt der Installation können Sie die Komponenten auswählen, die installiert werden sollen (Abbildung 3-5). Folgende Optionen stehen zur Verfügung:

- **Mentana CSP-Komponente:** Smart-CSP wird installiert
- **Office-Cryptor:** Installiert den Office-Cryptor, der das zertifikatsbasierte Ver- und Entschlüsseln beliebiger Dateien aus dem Kontext-Menü heraus erlaubt.
- **OfficeSigner:** OfficeSigner wird installiert.
- **Acrobat Plugin:** Installiert das Acrobat Plugin, welches ein bequemes Signieren aus dem Acrobat(-Reader) heraus ermöglicht.
- **Acrobat Reader Verifikation über die Windows-Zertifikatsverwaltung:** Stellt den Adobe Acrobat-Reader so ein, dass für die Unterschriftenverifikation die Windows-Zertifikatsverwaltung genutzt wird.

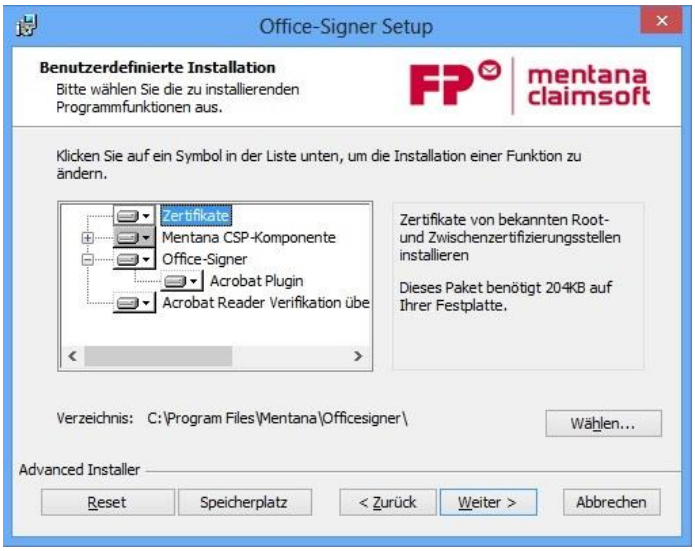

Abbildung 3-5 Installationsfenster mit benutzerdefinierter Installation

Abbildung 3-6 Vorbereitung Installation abgeschlossen

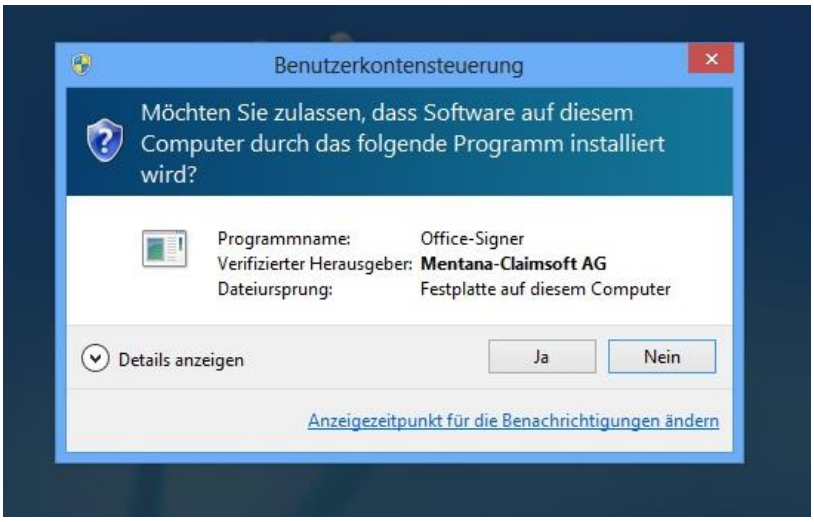

Abbildung 3-7 Abfrage Benutzerkontensteuerung Windows 7

3.1.4 INSTALLATIONSVERLAUF

Hier können sie den Verlauf der Installation des OfficeSigners verfolgen (Abbildung 3-8). Es wird angezeigt welche Dateien auf Ihr System kopiert und welche Verknüpfungen angelegt werden.

Abbildung 3-8 Installationsverlauf

3.1.5 ENDE DER INSTALLATION

Nun ist es geschafft und das Einrichten des OfficeSigners ist abgeschlossen (Abbildung 3-9). Durch klicken auf Fertigstellen wird das Installationsprogramm beendet. Sie können Sie den OfficeSigner jetzt verwenden.

Abbildung 3-9 Installationsende

3.2 LIZENZIERUNG DES OFFICESIGNER

Die Verwendung des OfficeSigners setzt den Besitz eines gültigen Lizenzschlüssels voraus. Diesen erhalten Sie entweder als Bestandteil des gelieferten Softwarepaketes oder auf Anfrage von der Mentana-Claimsoft GmbH. Falls Sie zum Zeitpunkt der Installation keine Lizenz-Datei besitzen, kontaktieren Sie bitte info@mentana-claimsoft.de. Sie erhalten daraufhin entweder ihre endgültige Lizenzierung bzw. Evaluationsschlüssel, dessen Gültigkeit auf 30 Tage beschränkt ist[4].

Beim ersten Start der Anwendung werden Sie aufgefordert ihren Lizenzschlüssel zu importieren. Wählen Sie im erscheinenden Hinweisfeld die Option Lizenzieren aus. Daraufhin wird der Lizenzmanager gestartet, welcher Ihnen das Importieren Ihrer Schlüsseldatei ermöglicht. Klicken Sie die Schaltfläche Öffnen an und wählen Sie den Speicherort der Lizenz-Datei aus (Abbildung 3-11). Klicken Sie anschließend erneut Öffnen. Das Fenster Lizenzmanager zeigt Ihnen daraufhin die Gültigkeitsinformationen der importierten Lizenz an.

[4] Die Art des gelieferten Schlüssels hängt vom Status Ihrer Bestellung ab

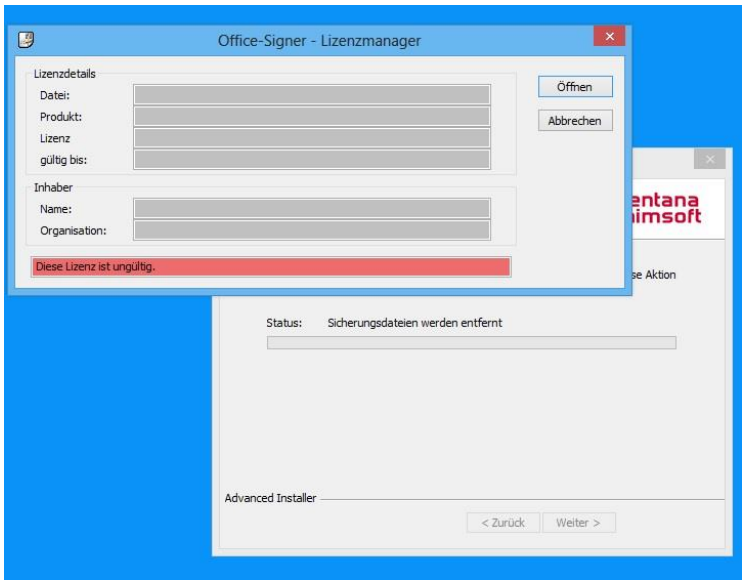

Abbildung 3-10 Noch keine, bzw. ungültige Lizenz

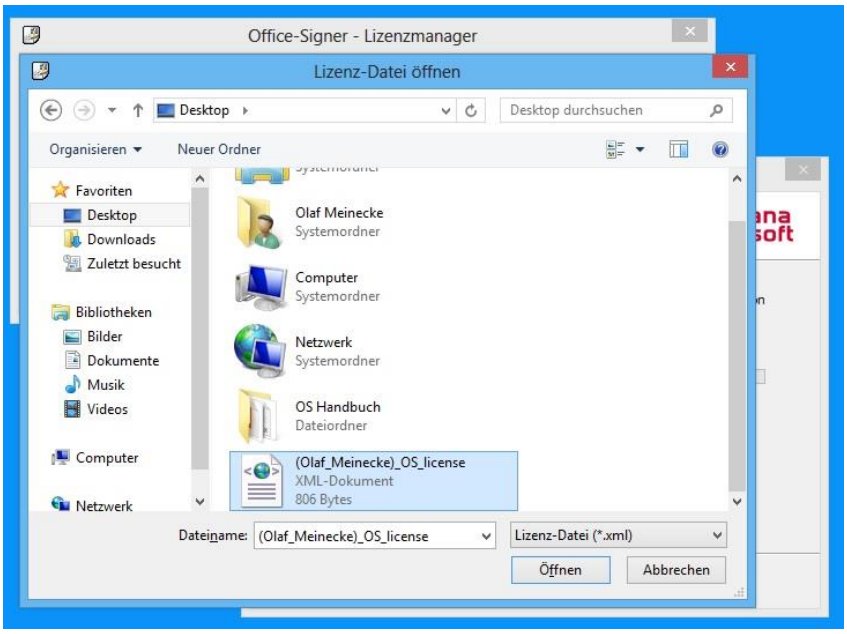

Abbildung 3-11 Lizenz-Datei öffnen

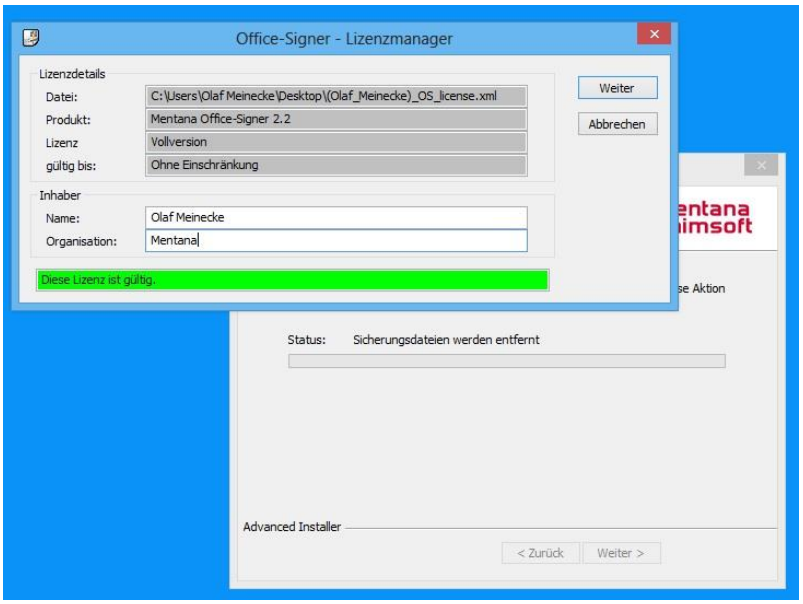

Abbildung 3-12 gültige Lizenz

3.3 INSTALLATION SOFTWAREZERTIFIKAT (OPTIONAL)

Bevor Sie sämtliche Funktionen des OfficeSigners nutzen können, benötigen Sie ein Signaturzertifikat. Dieses dient als elektronische Identität bei der Signatur (Unterzeichnung) von Dokumenten. Verfügen Sie bereits über ein Smartcard-Lesegerät und eine Signaturkarte, so können Sie den folgenden Abschnitt überspringen.

Auf Anforderung erhalten Sie zusammen mit Ihrer Version des OfficeSigners ein von der Mentana-Claimsoft GmbH ausgestelltes Softwarezertifikat. Bevor Sie dieses allerdings in der Signaturanwendung verwenden können, müssen Sie es in den Windows-Zertifikatspeicher installieren. Sichern Sie die Zertifikatsdatei `cert_ihr_name.p12` in ein beliebiges Verzeichnis. Öffnen Sie durch Rechtsklick auf diese Datei das zugehörige Kontext-Menü (Abbildung 3-13) und wählen Sie die Funktion PFX Installieren aus.

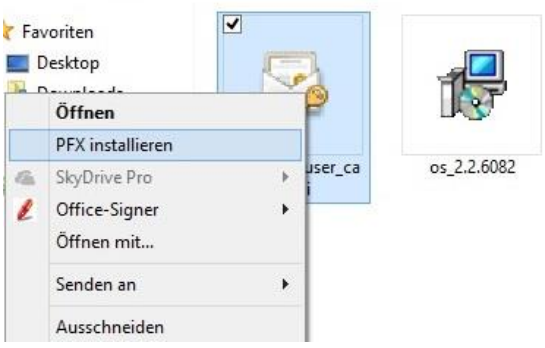

Abbildung 3-13 Softwarezertifikat installieren (Kontextmenü)

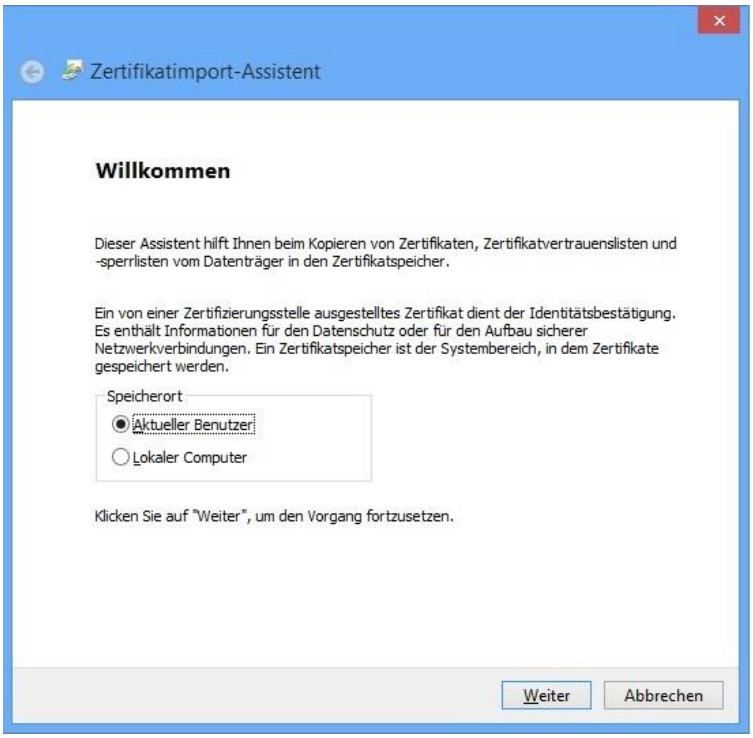

Abbildung 3-14 Zertifikatsimport – Willkommen

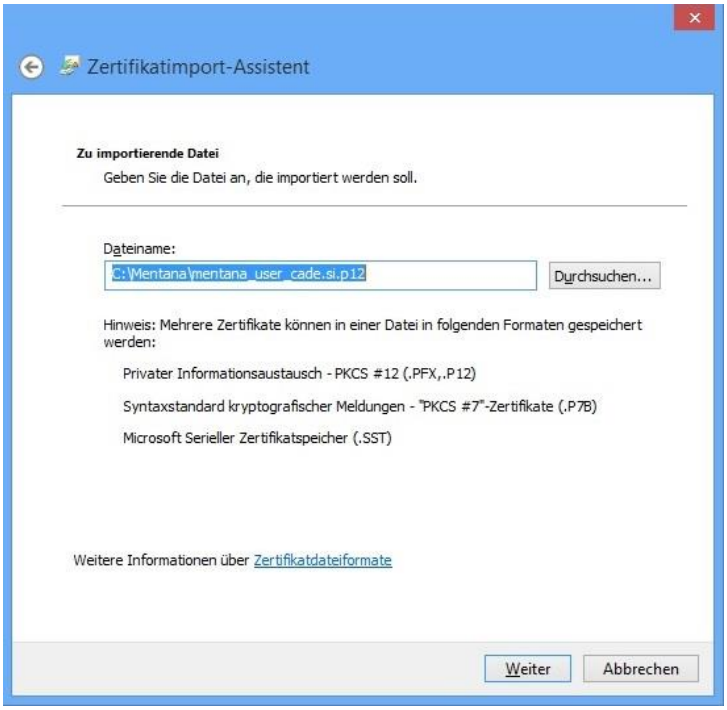

Abbildung 3-15 Zertifikatimport-Assistent

Windows wird Sie während des Importvorgangs (Abbildung 3-14) nach dem Passwort für den privaten Schlüssel fragen (Abbildung 3-16). Dieses lautet für alle von der Mentana-Claimsoft GmbH gelieferten Testzertifikate `Mentana` (groß und Kleinschreibung beachten).

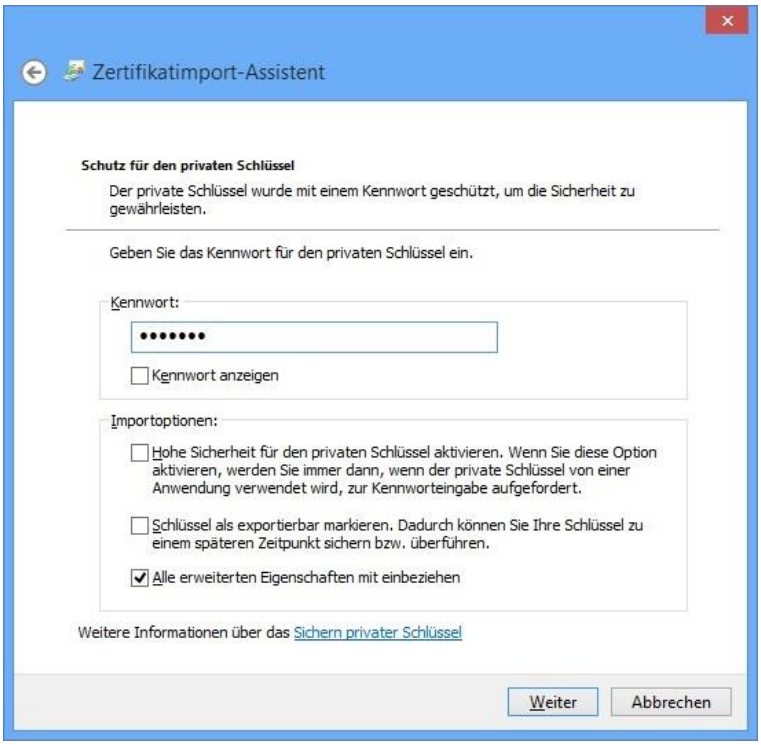

Abbildung 3-16 Zertifikatsimport – Kennworteingabe

Achten Sie während des Installierens darauf, dass Ihr Zertifikat in den Speicher Eigene Zertifikate installiert wird. Im Zweifelsfall wählen Sie die Option Zertifikatsspeicher automatisch auswählen (Abbildung 3-17).

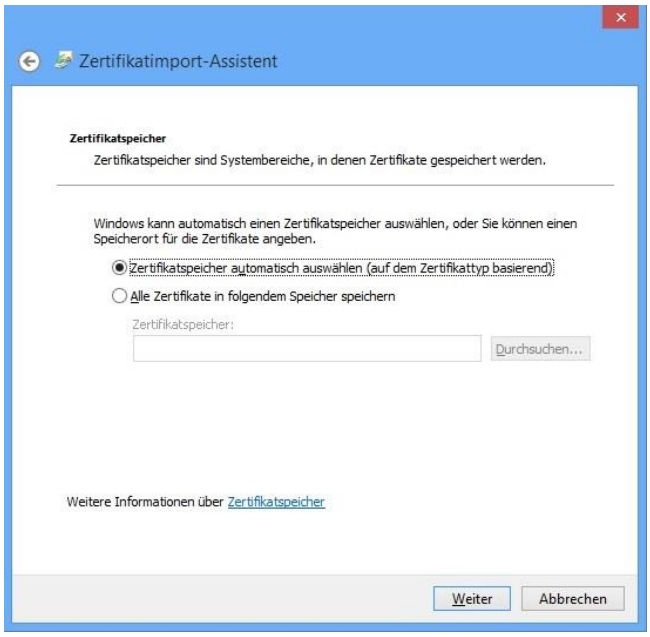

Abbildung 3-17 Zertifikatsimport – Zertifikatsspeicher

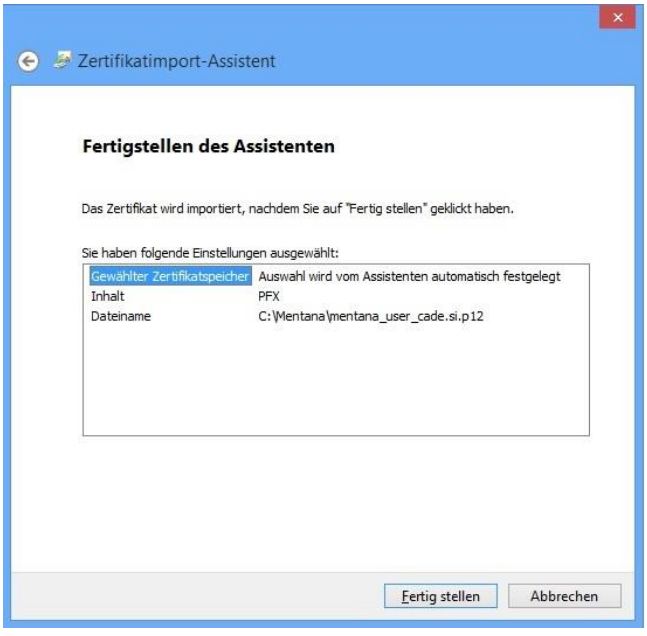

Abbildung 3-18 Zusammenfassung Zertifikatimport-Assistent

Die von der Mentana-Claimsoft gelieferten Software-Zertifikate enthalten auch die Stammzertifikate, der gesamten Kette.

Falls Sie die Stammzertifikate manuell nachinstallieren müssen, sorgen Sie für eine korrekte Zuordnung der Zertifikate zu den Zertifizierungsstellen:

Mentana Root 2010CA → Vertrauenswürdige Stammzertifizierungsstellen

Mentana User 2010CA →Zwischenzertifizierungsstellen

Bei der Installation des Stammzertifikates werden Sie speziell noch gefragt, ob Sie das Zertifikat `Mentana Root 2010 CA` der Liste der vertrauenswürdigen Stammzertifikate hinzufügen wollen. Beantworten Sie diese Frage mit Ja (Abbildung 3-19).

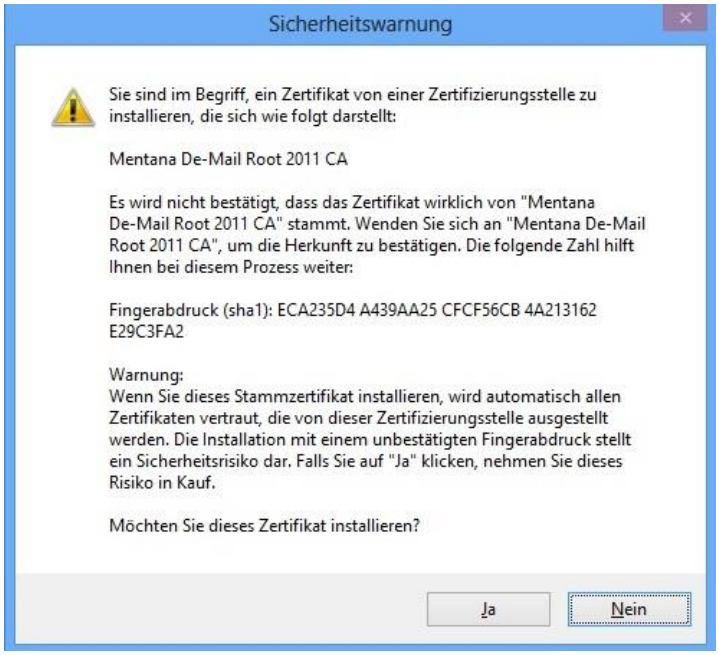

Abbildung 3-19 Zertifikatsimport – Sicherheitswarnung

Abbildung 3-20 Meldung einer erfolgreichen Zertifikats-Installation

3.4 EINSATZEMPFEHLUNGEN

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

- Verwenden Sie nur zugelassene Kartenleser und Signaturkarten (siehe auch Kapitel *Systemvoraussetzungen*)
- Halten Sie die PIN Ihrer Signaturkarte in jedem Fall geheim
- Verwenden Sie auf dem Signatursystem eine Zugangskontrolle unter Verwendung sicherer Passworte
- Überprüfen Sie Ihr Signatursystem regelmäßig auf bekannte Sicherheitslücken[5]
- Installieren Sie regelmäßig die vom Betriebssystemhersteller zur Verfügung gestellten Sicherheitsupdates[6]
- Installieren Sie einen Virenscanner[7]
- Sichern Sie Ihr Netzwerk gegen Eindringlinge durch den Einsatz einer Personal Firewall
- Installieren Sie ein Anti-Spyware-Programm[8]
- Verifizieren Sie die Integrität des OfficeSigner-Installationspaketes

3.5 ÜBERPRÜFEN DER KORREKTHEIT DER INSTALLATION

Der Hersteller hat alle Komponenten des OfficeSigner unter Verwendung einer Code-Signatur gegen versehentliche oder vorsätzliche Veränderungen geschützt. Bitte vergewissern Sie sich in regelmäßigen Abständen von der Korrektheit Ihrer Installation.

Zum Prüfen der Installation gehen Sie wie folgt vor:

1. Öffnen Sie den Installationsordner des OfficeSigner im Windows Explorer
2. Klicken Sie die Datei `OfficeSignerWx.exe` an und wählen aus dem Kontext-Menü die Funktion Eigenschaften aus.
3. Wechseln Sie auf die Seite Digitale Signaturen
4. Wählen Sie die Signatur aus und klicken Sie auf Details.
5. Der Explorer zeigt Ihnen an, ob die Signatur weiterhin korrekt ist und ob Sie von der Mentana-Claimsoft GmbH ausgestellt wurde. Überprüfen Sie insbesondere, ob

[5] Hierfür benötigte Programme finden Sie beispielsweise unter www.bsi.de
[6] Diese finden Sie unter www.windowsupdate.com
[7] Eine für den privaten Einsatz kostenfreie Version finden Sie z.B. unter www.avira.de
[8] Beispielsweise Microsoft Anti Spyware, Download unter www.microsoft.com

a. Die Integrität der Anwendung weiterhin gegeben ist
b. Ob das Unterzeichner-Zertifikat auf die Mentana-Claimsoft AG[9] ausgestellt wurde
c. Ob die Glaubwürdigkeit des Zertifikates durch die GeoTrust TrustCenter CodeSigning CA I bestätigt wurde.

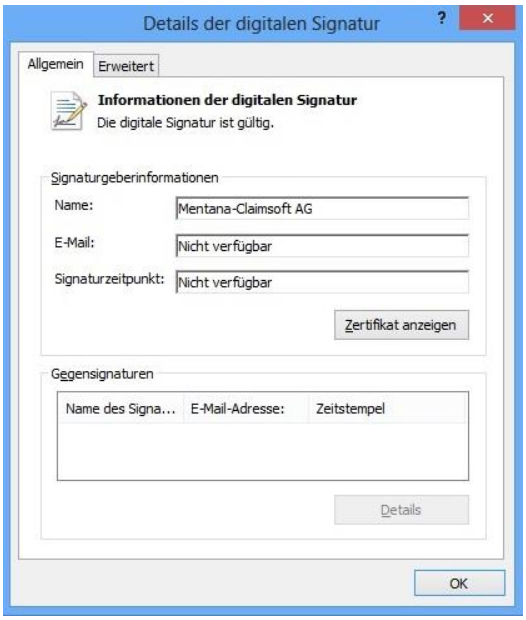

Abbildung 3-21 Details der digitalen Signatur

4 VERWENDEN DES OFFICESIGNERS

4.1 ERSTELLEN ELEKTRONISCHER SIGNATUREN

In Abhängigkeit vom Typ des zu unterzeichnenden Dokumentes unterstützt der OfficeSigner 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 nur für Dokumente im PDF-Format zur Verfügung.
- **Externe Signatur:** Bei diesem Verfahren wird eine weitere Datei erzeugt, in der die kryptographischen Daten im PKC#S7-Format abgelegt werden. Bei diesem Verfahren benötigt der Empfänger das Ausgangsdokument und die Signaturdatei, um Urheber und Integrität eines empfangenen Dokumentes feststellen zu können.

[9] Im Zuge der Umfirmierung sind bei Drucklegung dieses Handbuchs noch nicht alle Code-Signing-Zertifikate auf die GmbH umgestellt.

4.1.1 ERSTELLEN EINER EINGEBETTETEN UNSICHTBAREN SIGNATUR (NUR PDF)

Öffnen Sie das Kontext-Menü der zu signierenden Datei und wählen Sie die Funktion Dokument signieren aus. Daraufhin werden Sie vom OfficeSigner aufgefordert, das zum Signieren zu verwendende Zertifikat auszuwählen (Abbildung 4-2). Zertifikate, die nicht zum Erstellen elektronischer Signaturen geeignet sind, werden durch ein vorangestelltes rotes Kreuz gekennzeichnet, verwendbare durch ein grünes Häkchen. Sie können diesen Dialog weiterhin verwenden, um die folgenden Aktivitäten auszuführen:

- Schaltfläche Zertifikate aktualisieren: der Zertifikatsspeicher wird neu eingelesen
- Schaltfläche Zertifikat anzeigen: Ermöglicht die Anzeige zusätzlicher Informationen zum ausgewählten Zertifikat (Abbildung 4-1). Das Signaturgesetz empfiehlt die Überprüfung des verwendeten Zertifikates vor Ausführung jedes Signaturvorganges.
- Schaltfläche Dokument anzeigen: Ermöglicht die Anzeige des Dokumentes, welches Sie im nächsten Schritt unterschreiben werden. Das Signaturgesetz empfiehlt die Überprüfung der zu signierenden Daten vor jedem Signaturvorgang.

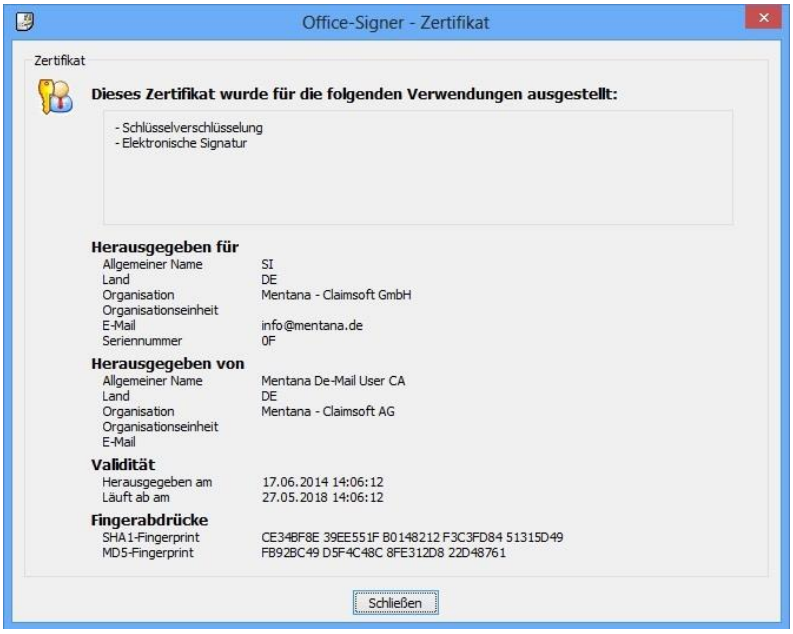

Abbildung 4-1 Infos über Zertifikat

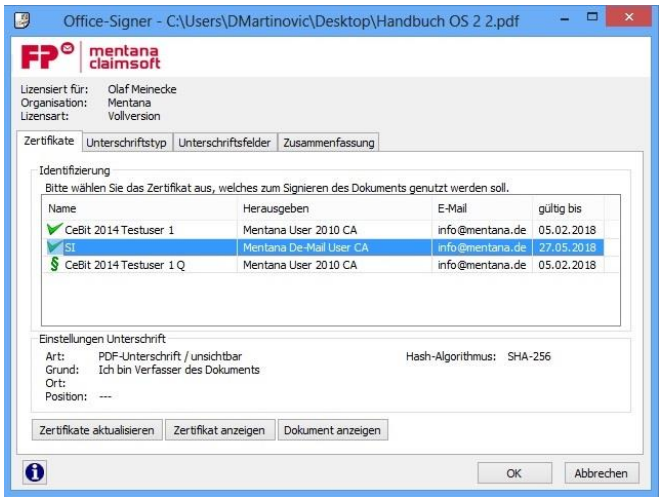

Abbildung 4-2 Zertifikat auswählen

Auf der nächsten Registerkarte des Dialogs (Abbildung 4-3) können Sie festlegen, welche Art von Unterschrift Sie verwenden wollen. Bei PDF-Dokumenten stehen Ihnen vier Möglichkeiten zur Verfügung (Abbildung 4-4).

- Eingebettete PDF-Unterschrift / unsichtbar
- Eingebettete PDF-Unterschrift / sichtbar
- Externe S/MIME-Signatur
- Eingebettete S/MIME Signatur

Wählen Sie Eingebettete PDF-Unterschrift / unsichtbar.

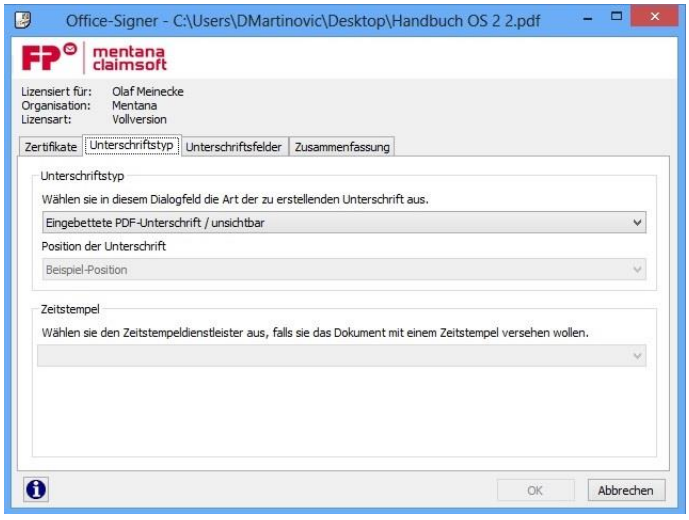

Abbildung 4-3 Unterschriftstyp

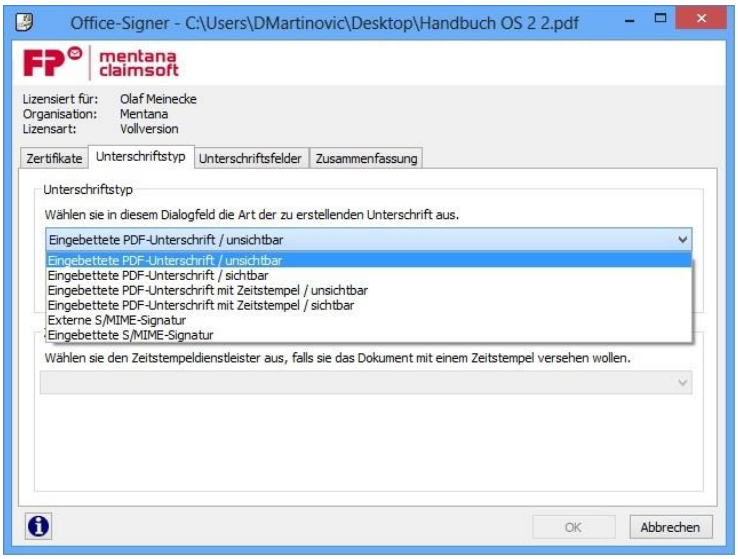

Abbildung 4-4 Unterschriftstyp auswählen

Das Eingabefeld Unterschriftsposition wird nur aktiv, wenn Sie eine sichtbare Unterschrift erstellen wollen.

Auf der Registerkarte Unterschriftsfelder (Abbildung 4-5) besteht die Möglichkeit der Eingabe des Grundes der Dokumentunterzeichnung und des Ortes. Grund und Ort der Unterschrift können Sie frei definieren und ein Standardwert festlegen. Sie können die Auswahlliste (Abbildung 4-6 und Abbildung 4-7) verwenden oder die Vorgaben auch einfach überschreiben, wenn Sie eine andere Begründung oder einen anderen Ort für Ihre Unterschrift verwenden wollen. Falls Sie die Optionen Eingaben im Feld "Begründungen" automatisch in Konfiguration übernehmen oder Eingaben im Feld "Ort" automatisch in Konfiguration übernehmen eingeschaltet haben werden Ihre Eingaben automatisch gespeichert und stehen beim nächsten Signieren als Auswahl zur Verfügung (siehe dazu auch Kapitel 5.2).

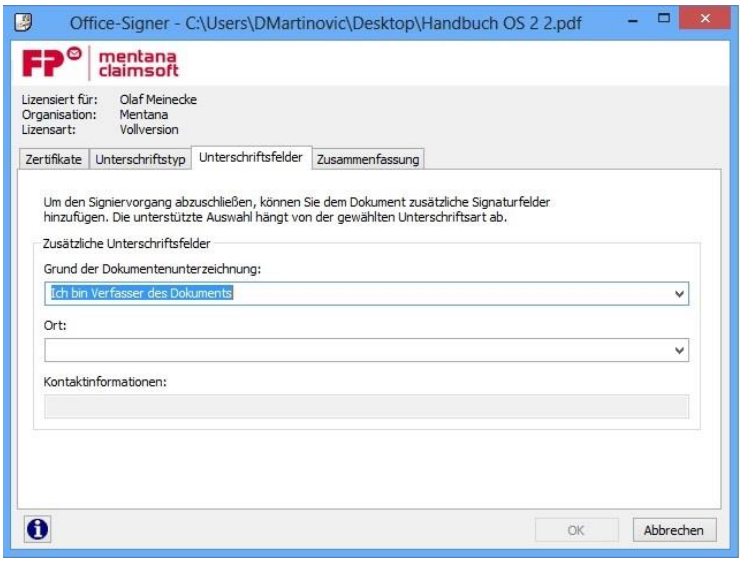

Abbildung 4-5 Unterschriftsfelder

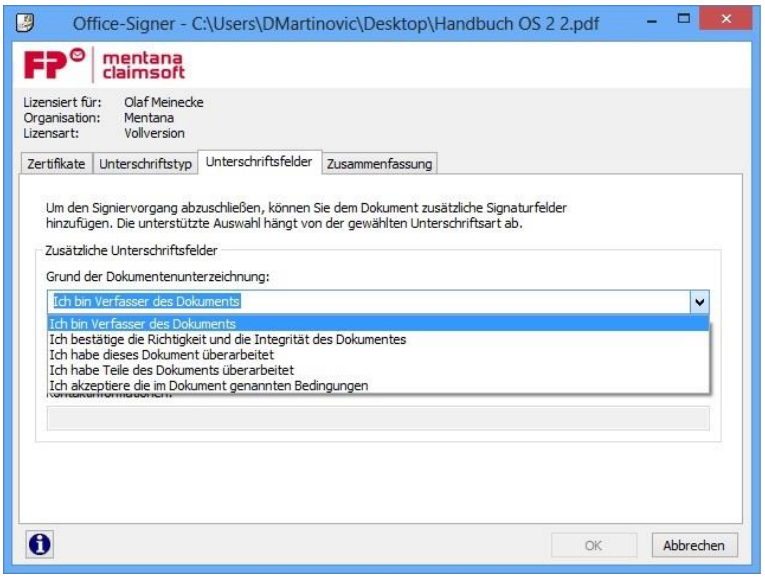

Abbildung 4-6 Begründung auswählen

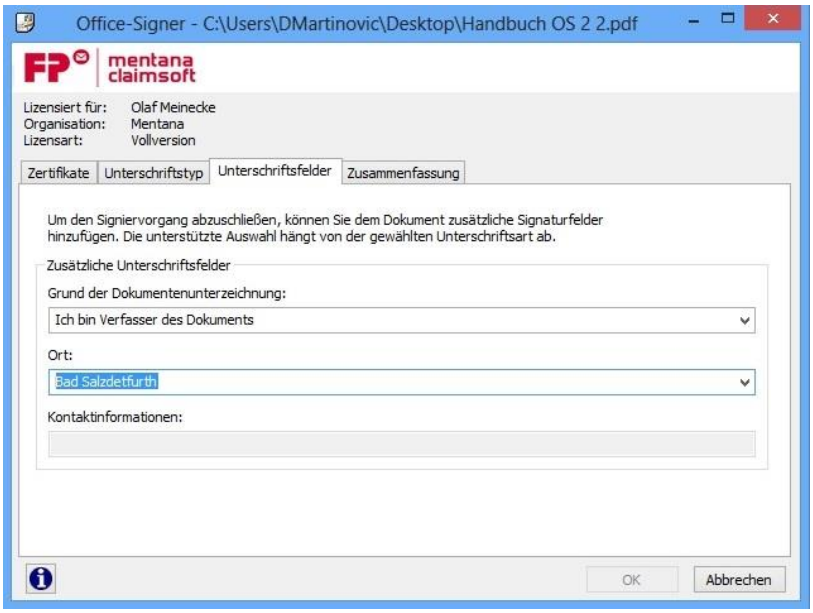

Abbildung 4-7 Ort auswählen

Auf der letzten Registerkarte (Abbildung 4-8) werden alle vorgenommenen Einstellungen angezeigt. Sie können folgende Funktionen aufrufen:

- **Zertifikat anzeigen:** zeigt das ausgewählte Zertifikat an
- **Dokument anzeigen:** zeigt das zur Unterschrift ausgewählte Dokument an
- **Speichern unter:** speichert das unterschriebene Dokument unter einem anderen Namen

Klicken Drücken Sie auf OK, wenn Sie das Dokument mit den aktuellen Einstellungen unterzeichnen wollen. Durch Klicken auf Abbrechen wird der Dialog beendet und das Dokument wird *nicht* unterzeichnet.

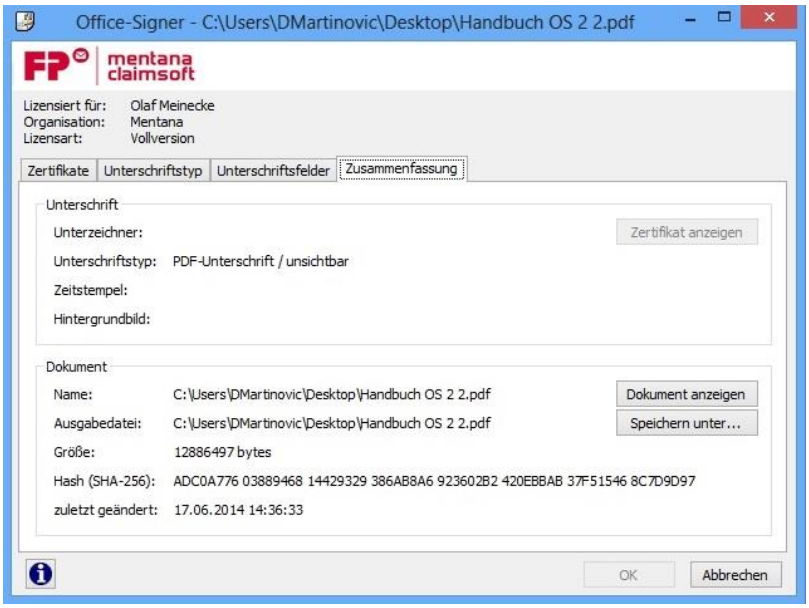

Abbildung 4-8 Zusammenfassung für die Unterschrift

Abbildung 4-9 Signaturwarndialog

Nach erfolgreicher Signierung des Dokumentes erhalten Sie eine Bestätigung (Abbildung 4-10). Im Falle eines Fehlers erhalten Sie eine genaue Fehlermeldung.

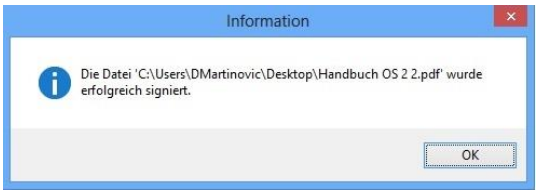

Abbildung 4-10 Bestätigung bei erfolgreicher Unterschrift

Öffnen Sie nun das signierte PDF-Dokument, um sich die Unterschrift anzuschauen (Abbildung 4-11). Wenn Sie die Option Dokument nach erfolgreicher Signatur öffnen ausgewählt haben, wird das signierte Dokument automatisch geöffnet.

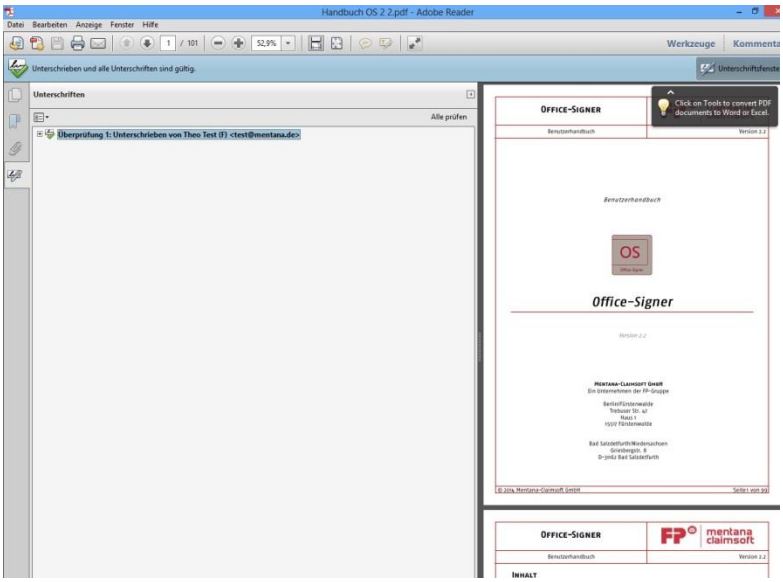

Abbildung 4-11 Unterschrift im PDF-Dokument (Ansicht Adobe PDF-Reader)

4.1.2 ERSTELLEN EINER EINGEBETTETEN SICHTBAREN SIGNATUR (NUR PDF)

Öffnen Sie das Kontext-Menü der zu signierenden Datei und wählen Sie die Funktion Dokument signieren aus. Daraufhin werden Sie vom OfficeSigner aufgefordert, das zum Signieren zu verwendende Zertifikat auszuwählen (Abbildung 4-12).

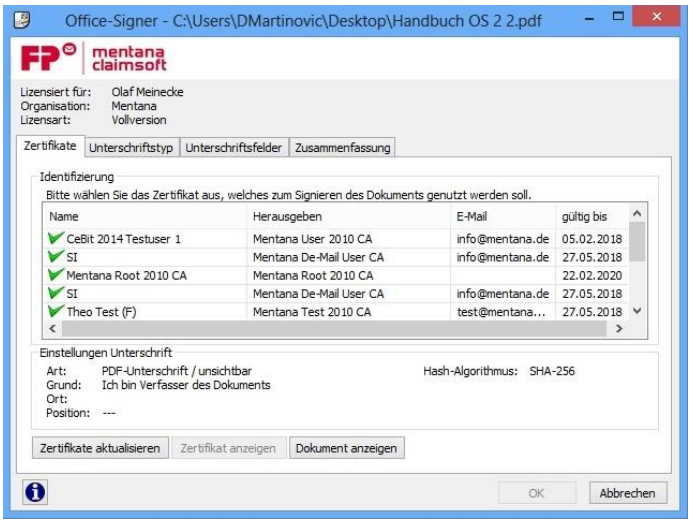

Abbildung 4-12 Zertifikat auswählen für Signatur

Wählen Sie nun auf dem Registerblatt Unterschriftstyp den Typ Eingebettete PDF-Unterschrift / sichtbar aus (Abbildung 4-13). Nach erfolgter Auswahl wird das Feld Position der Unterschrift zum Bearbeiten freigegeben. Wählen Sie eine Position aus der Liste der verfügbaren Unterschriftspositionen aus. Wenn noch keine Unterschriftsposition in der Auswahlliste vorhanden ist, müssen Sie erst eine Position für die Unterschrift festlegen. Dazu rufen Sie die Einstellungen des OfficeSigners auf. Die Unterschriftsposition legt fest, auf welcher Seite und an welcher Stelle des Dokumentes sich die sichtbare Unterschrift befinden soll. Es ist auf möglich eine Bild (z.B. eine eingescannte Unterschrift) als sichtbare Unterschrift zu verwenden.

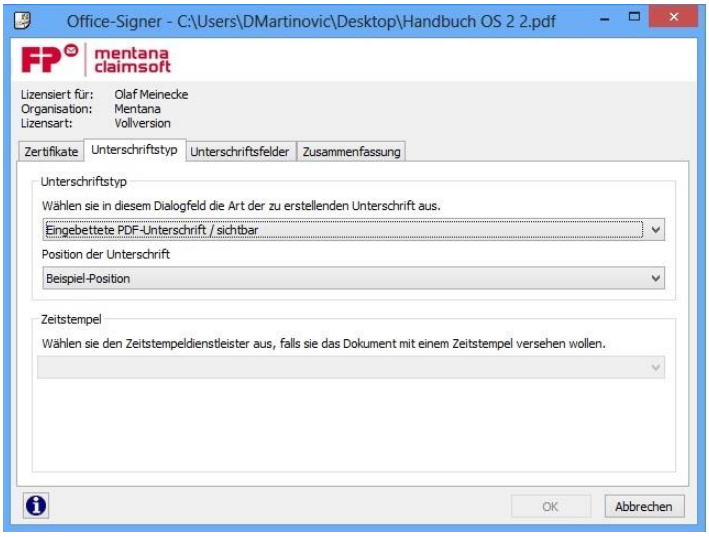

Abbildung 4-13 Unterschriftstyp und Unterschriftsposition selektieren

Der weitere Ablauf des Signierens ist identisch mit dem der unter Abschnitt 4.1.1 beschrieben wurde. Sie wählen eine Begründung und einen Ort aus (Abbildung 4-14) überprüfen alle Einstellungen (Abbildung 4-15) und starten das Signieren durch Klicken auf OK. Nach erfolgreichem Signieren des PDF-Dokuments erhalten Sie wieder eine Bestätigung (Abbildung 4-17).

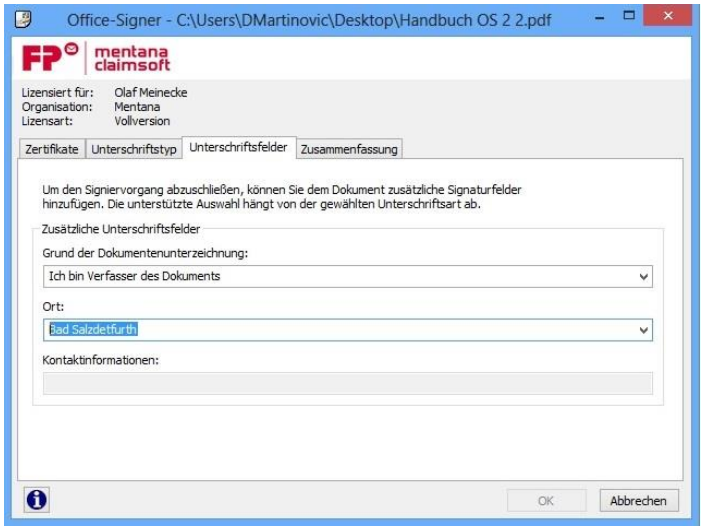

Abbildung 4-14 Begründung und Ort der Signatur

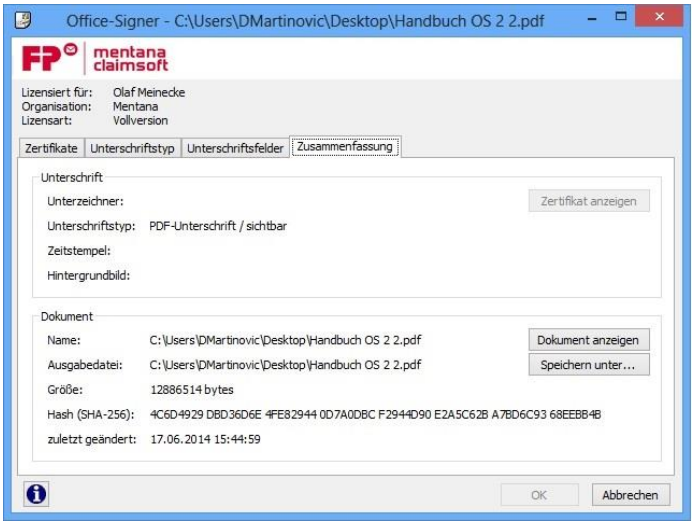

Abbildung 4-15 Zusammenfassung zur eingebetteten, sichtbaren Signatur

Abbildung 4-16 Signaturwarndialog vor Signatur

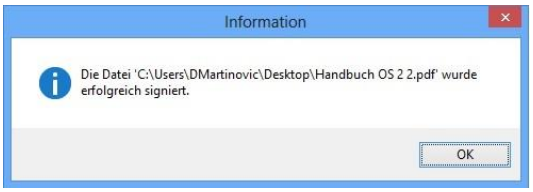

Abbildung 4-17 Bestätigung nach erfolgter Signatur

Falls Sie den OfficeSigner so konfiguriert haben, dass das Dokument nach erfolgreicher Unterschrift *nicht* angezeigt werden soll, öffnen Sie das unterschriebene PDF-Dokument. Navigieren Sie auf die Seite des Dokumenten, auf der die Unterschrift positioniert werden sollte. Sie werden eine Grafik an der entsprechenden Stelle finden (Abbildung 4-18). Mit einem Klick auf diese Grafik können Sie die Unterschrift prüfen und deren Eigenschaften anzeigen.

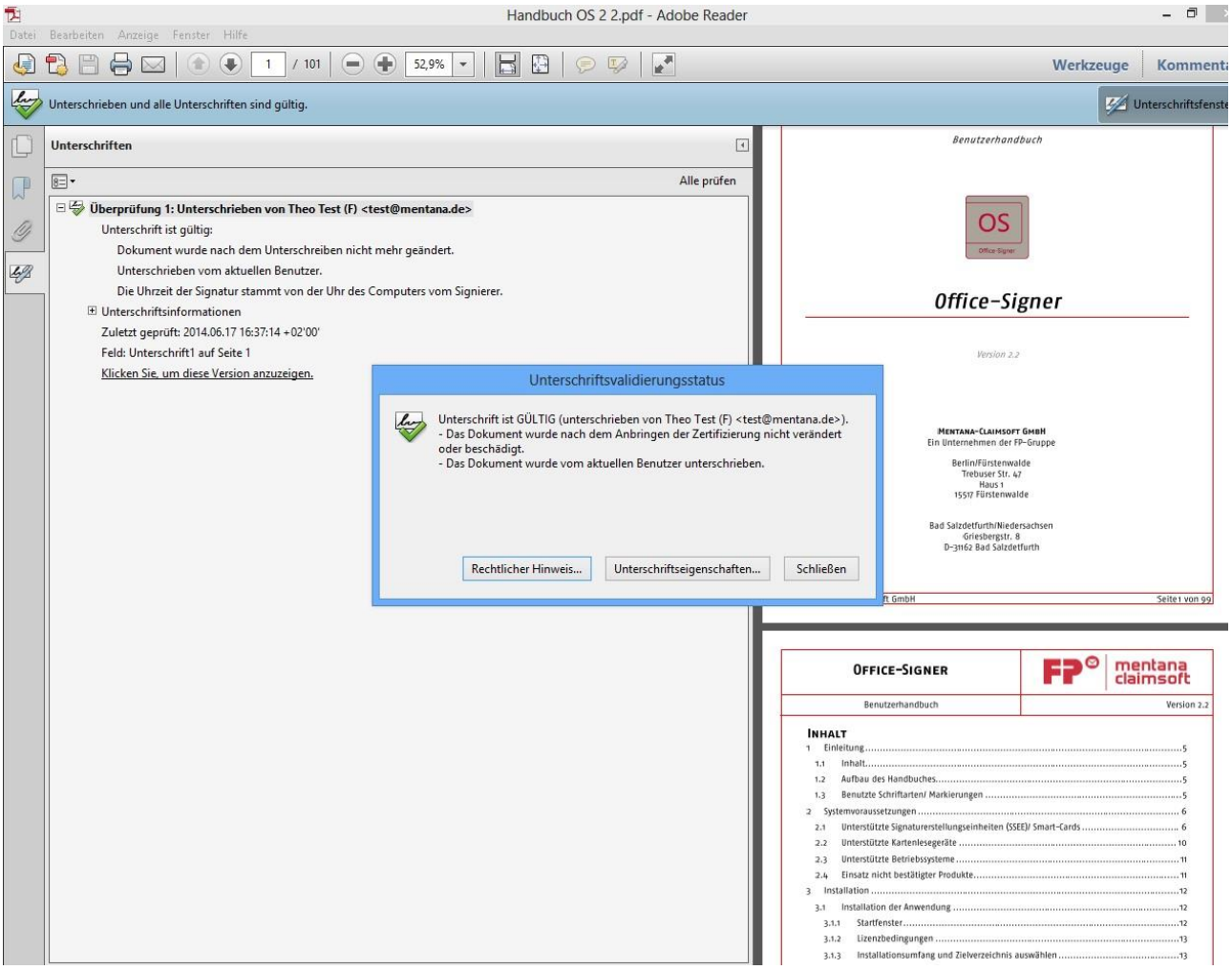

Abbildung 4-18 sichtbare Unterschrift im PDF-Dokument (Ansicht Adobe PDF-Reader)

4.1.2.1 POSITIONIERUNG AUSSEHEN

Sie können das Aussehen und die Position einer sichtbaren Signatur konfigurieren (siehe Kapitel 5.6). Sobald Sie nun eine sichtbare Signatur erstellen wollen, können Sie aus den verschiedenen Konfigurationen die Gewünschte wählen.

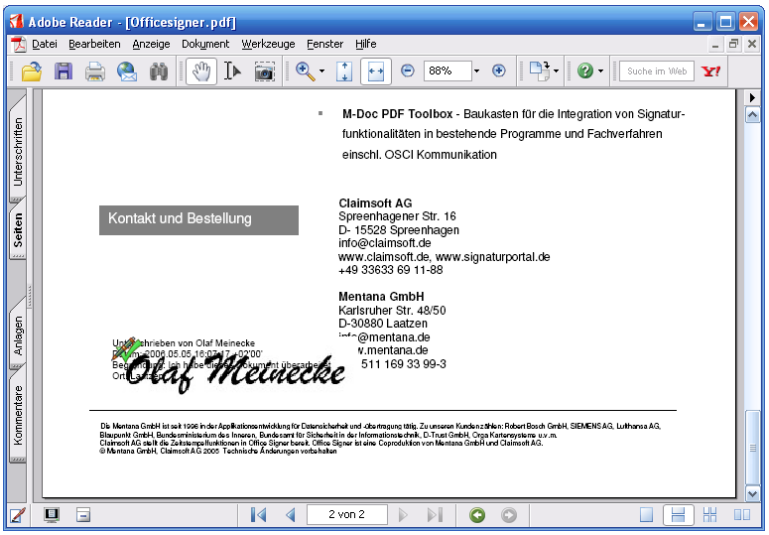

Abbildung 4-19 sichtbare Unterschrift mit Hintergrundbild in PDF-Dokument

4.1.3 ERSTELLEN EINER EXTERNEN ODER EINGEBETTETEN S/MIME SIGNATUR

Wenn Sie Dokumente signieren wollen, die nicht im PDF-Format vorliegen (z.B.: Word, Open Office, TIFF...) dann können Sie das mit Hilfe einer externen oder eingebetteten S/MIME Signatur tun. Dabei wird eine Datei mit der Erweiterung `p7s` bzw. `p7m` angelegt, in der die Unterschrift enthalten ist. Die p7s Datei beinhaltet nur die Signatur zu dem Dokument (extern) wogegen die p7m Dateien Signatur und Dokument enthält (eingebettet). Natürlich können Sie auch PDF-Dokumente extern signieren.

Um ein Dokument extern zu signieren gehen Sie wie folgt vor: Öffnen Sie das Kontext-Menü der zu signierenden Datei und wählen Sie die Funktion Dokument signieren aus dem OfficeSigner-Menü aus. Wählen Sie das Zertifikat aus, mit dem Sie das Dokument unterzeichnen wollen (Abbildung 38). Wenn Sie ein beliebiges Dokument signieren wollen, ist bereits Externe S/MIME Signatur ausgewählt (Abbildung 39). Falls Sie ein PDF-Dokument extern signieren wollen, müssen Sie erst noch Extern S/MIME Signatur oder Eingebettete S/MIME Signatur auswählen. Bei einer externen Signatur besteht keine Möglichkeit eine Begründung und einen Ort der Unterschrift zu hinterlegen. Darum sind die Eingabefelder auf der Registerkarte Unterschriftsfelder auch deaktiviert.

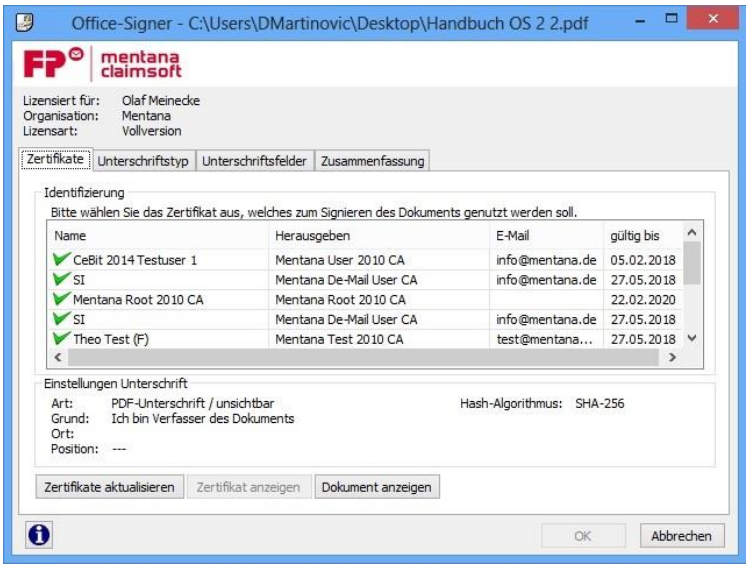

Abbildung 4-20 Zertifikat auswählen

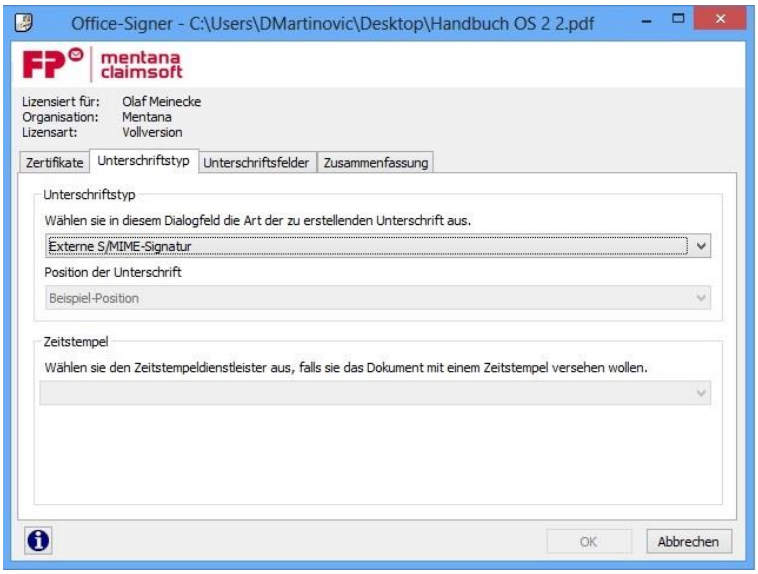

Abbildung 4-21 Unterschriftstyp wählen

Auf dem Registerblatt Zusammenfassung können Sie Ihre Einstellungen überprüfen, das Zertifikat anzeigen, das Dokument anzeigen und den Dateinamen der Signaturdatei festlegen (Abbildung 4-22).

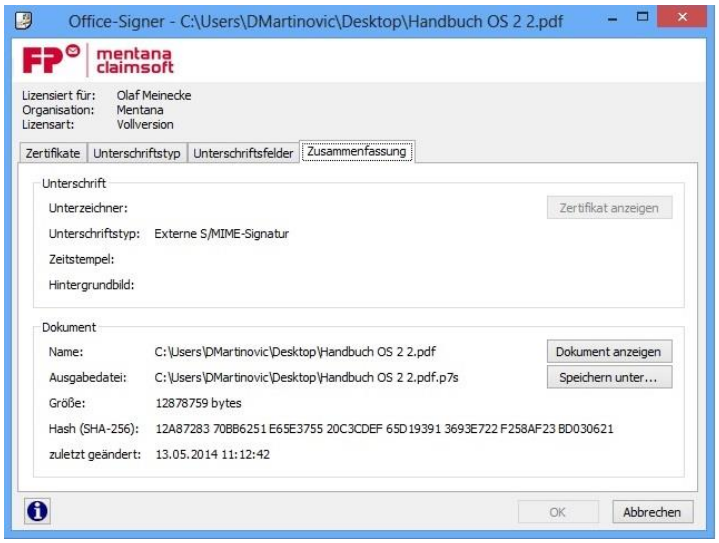

Abbildung 4-22 Zusammenfassung

Abbildung 4-23 Signaturwarndialog

Nach erfolgreichem Signieren erhalten Sie die gewohnte Bestätigungsmeldung (Abbildung 4-24).

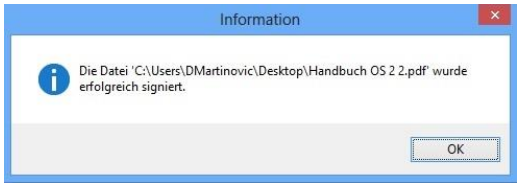

Abbildung 4-24 Bestätigung nach erfolgter Signatur

Die Unterschrift wird in einer P7S-Datei abgelegt (Abbildung 4-25).

Abbildung 4-25 Dateiliste mit externer Signatur

4.1.4 ERSTELLEN VON STAPELSIGNATUREN

Wenn Sie mehrere Dateien gleichzeitig signieren möchten, markieren Sie die gewünschten Dateien und öffnen Sie das Kontextmenü. Dies geschieht entweder mit Hilfe der rechten Maustaste oder der Tastenkombination UMSCHALTTASTE+F10. Im sich öffnenden Kontext-Menü erhalten Sie Zugang zu sämtlichen Funktionen des Office-Singers. Um die Dokumente zu signieren gehen Sie wie folgt vor: Öffnen Sie das Kontext-Menü und wählen Sie die Funktion Dokumente signieren aus dem OfficeSigner Menü aus. Wählen Sie das Zertifikat aus, mit dem Sie das Dokument unterzeichnen wollen. Auf dem Registerblatt Dateiliste sind die ausgewählten Dateien aufgelistet (Abbildung 4-26). Hier können Sie weitere Dateien hinzufügen oder wieder entfernen. Wenn Sie eine Datei markieren und auf Bearbeiten klicken, öffnet sich ein neues Dialogfeld. Hier können Sie die Signatureinstellungen für PDF-Dokumente (Abbildung 4-27) und nicht PDF-Dokumente (Abbildung -46) bearbeiten. Durch Anklicken des OK-Buttons werden die Änderungen übernommen.

Um den Signiervorgang abzuschließen, klicken Sie bitte wie gewohnt auf OK. Die Dokumente werden signiert und es erscheint ein Dialogfeld mit den Signaturergebnissen (Abbildung 4-30). Je nach verwendeter Signaturkarte müssen Sie die PIN einmalig oder pro Dokument eingeben.

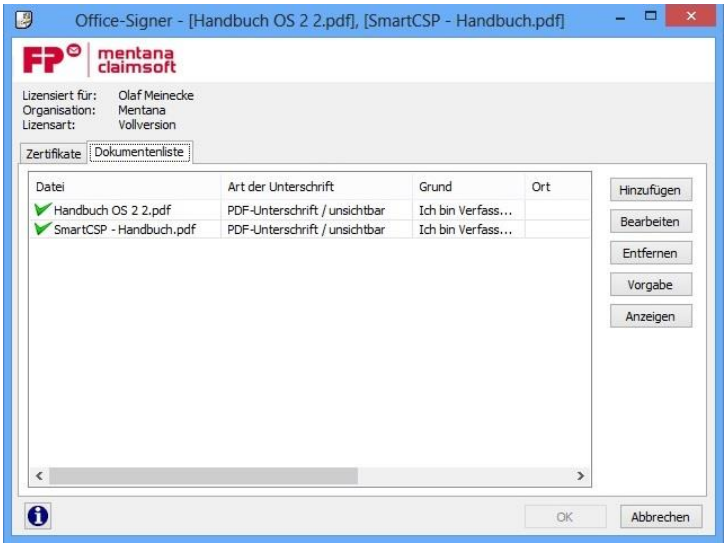

Abbildung 4-26 Dateiliste bei Stapelsignatur

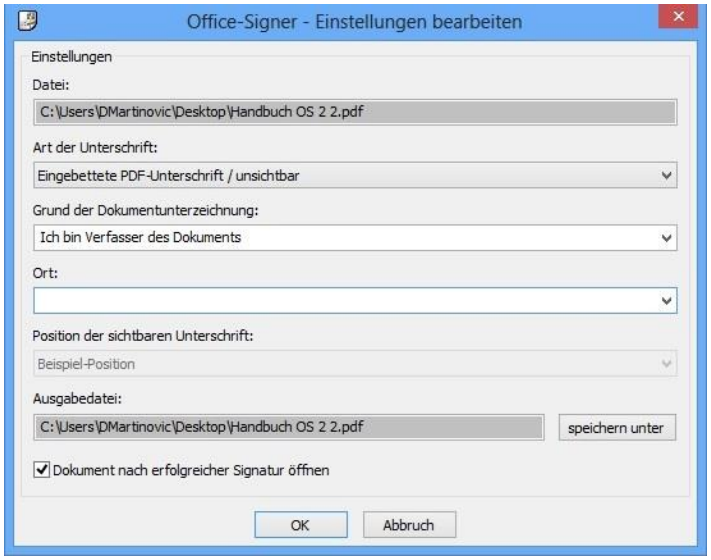

Abbildung 4-27 Einstellungen PDF-Dokumente

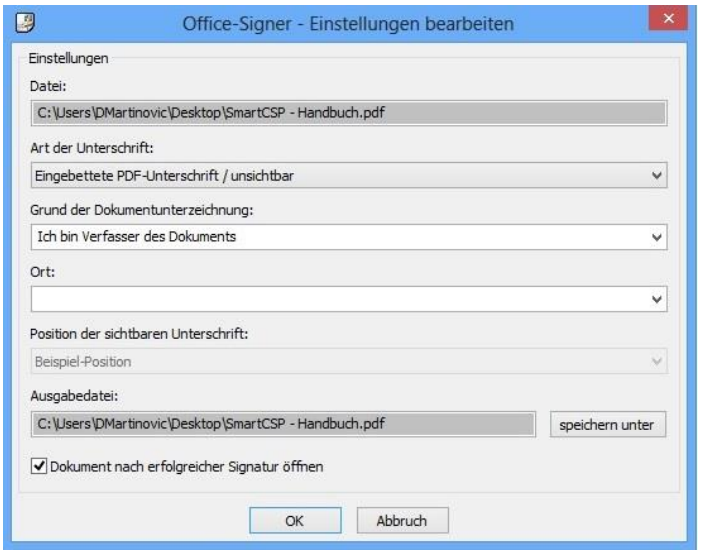

Abbildung 4-28 Einstellungen nicht PDF-Dokumente

Abbildung 4-29 Signaturwarndialog

Abbildung 4-30 Signaturergebnisse

4.2 VERIFIZIEREN ELEKTRONISCHER SIGNATUREN UND DE-MAILS

Der OfficeSigner ermöglicht es Ihnen, Signaturen zu beliebigen Dokumenten zu verifizieren. In Abhängigkeit vom Typ des zu überprüfenden Dokumentes werden zwei verschiedene Verifikationsmechanismen unterstützt:

- **Interne Signaturen:** Dieses Verifikationsverfahren wird bei Dokumenten verwendet, die eingebettete Mehrfachsignaturen unterstützen. Derzeit steht diese Option nur bei PDF-Dokumenten zur Verfügung.
- **Externe Signaturen:** Dieses Verifikationsverfahren setzt voraus, dass Sie im Besitz des Dokumentes und der zugehörigen Signaturdatei im PKCS#7-Format sind. Dieses Prüfverfahren ist bei beliebigen Datenformaten möglich.

Die Verifikation einer Unterschrift umfasst die Überprüfung der folgenden Punkte:

- **Integrität:** Ist der in der Signatur verschlüsselt abgelegte Hashwert mit dem aktuell berechneten Vergleichswert identisch?

- **Namensgleichheit:** Stimmt der in der Signatur als Unterzeichner angegebene Name mit dem Namen des Zertifikatsinhabers überein?
- **Zertifikatskette:** Kann, ausgehend vom Zertifikat des Unterzeichners, eine Liste der übergeordneten Zertifikate erstellt werden und beginnt diese Kette mit einem vertrauenswürdigen Stammzertifikat?
- **Zertifikatsgültigkeit:** Wurde die Unterschrift innerhalb des Gültigkeitszeitraumes der Zertifikatskette erstellt? Die Gültigkeit der Zertifikatskette kann nach zwei Prüfmodellen verifiziert werden:
  - Schalenmodell: Es wird überprüft, ob zum Zeitpunkt der Unterzeichnung sämtliche Zertifikate gültig waren ***(Nicht SigG-Konform!)***.
  - Kettenmodell: Es wird überprüft, ob das Unterzeichnerzertifikat zum Zeitpunkt der Signaturerstellung gültig war und ob sämtliche Zertifikate der Kette innerhalb des Gültigkeitszeitraumes des jeweils übergeordneten Zertifikates erstellt wurden.
- **Sperrlistenvermerke:** Wurde eines der Zertifikate der Zertifikatskette zum Zeitpunkt der Signaturerstellung auf einer Sperrliste des übergeordneten Trustcenters geführt? OfficeSigner wertet die im Zertifikat angegebenen Sperrlisten-Verteilungspunkte aus und lädt die benötigten Sperrlisten automatisch herunter. Aus diesem Anlass baut das Programm selbsttätig eine Internet-Verbindung zum Trustcenter auf

4.2.1 VERIFIZIEREN EINER EINGEBETTETEN SIGNATUR (NUR PDF)

Öffnen Sie das Kontext-Menü des zu verifizierenden PDF-Dokumentes und wählen Sie im OfficeSigner-Menü die Funktion Verifizieren (Abbildung 4-31). Die Fortschrittsanzeige (Abbildung 4-32) informiert Sie über den Stand der Verifikation.

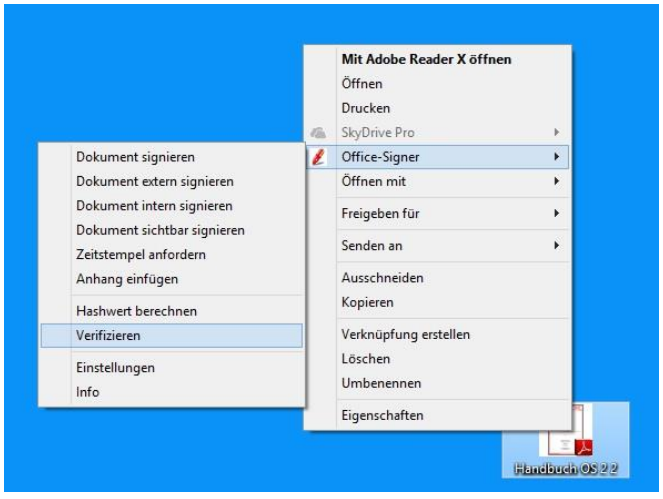

Abbildung 4-31 OfficeSigner - Menü – Verifizieren (Kontextmenü)

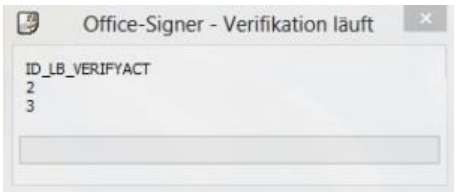

Abbildung 4-32 Fortschrittsanzeige Verifikation

Nach Beendigung der Verifikation erscheint ein Dialog mit der Liste der im PDF-Dokument enthaltenen Unterschriften und deren Gültigkeit (Abbildung 4-33). Sie können sich zu jeder Unterschrift Details (Abbildung 4-34) der Verifikation anzeigen lassen, indem Sie auf Details klicken. Mithilfe der Funktion Protokoll speichern wird das Ergebnis der Verifikation in eine XML – Datei gespeichert (Abbildung 4-35).

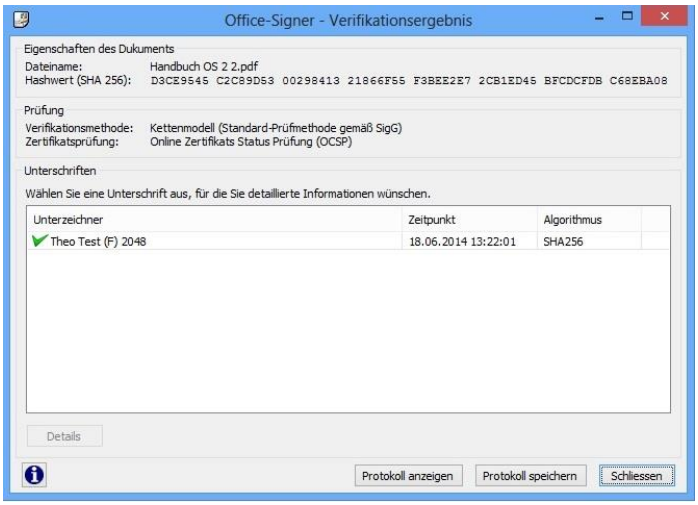

Abbildung 4-33 Verifikationsergebnis

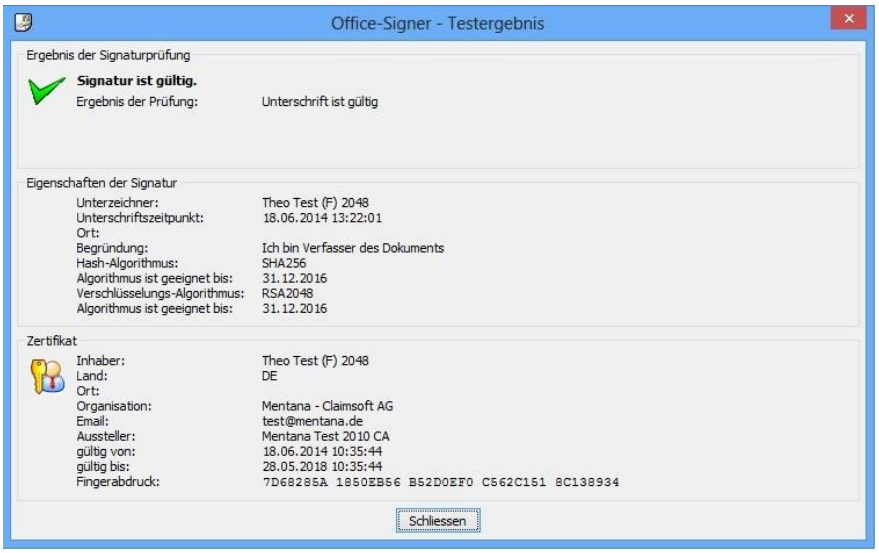

Abbildung 4-34 Testergebnis

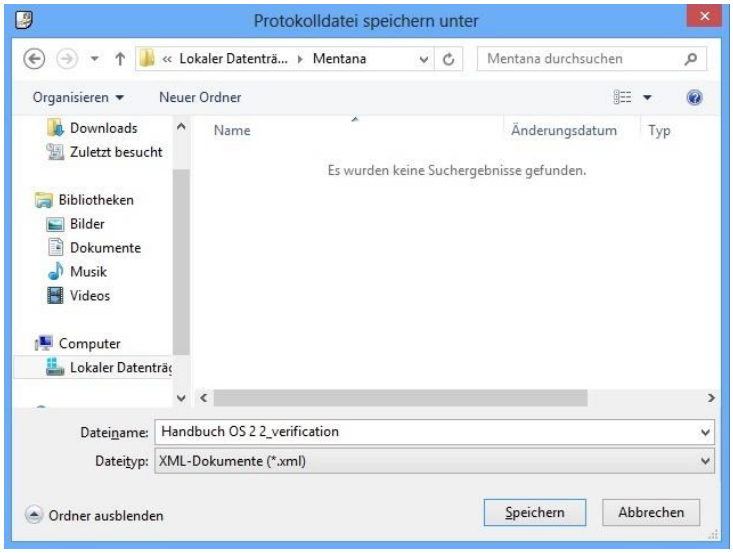

Abbildung 4-35 Protokoll speichern

Öffnen Sie die Protokolldatei, um weitere Informationen über die Verifikation zu erhalten (Abbildung 4-36 und Abbildung 4-41). Damit das Protokoll richtig angezeigt werden kann, benötigen Sie einen Internetzugang.

Abbildung 4-36 Dateiliste mit Verifikationsprotokoll

Für die Anzeige des Verifikationsprotokolls benötigen Sie die entsprechende xslt-Datei. Diese formatiert die Ausgaben. Haben Sie diese Datei nicht in ihrem Verzeichnis, so sieht das Ergebnis wie folgt aus:

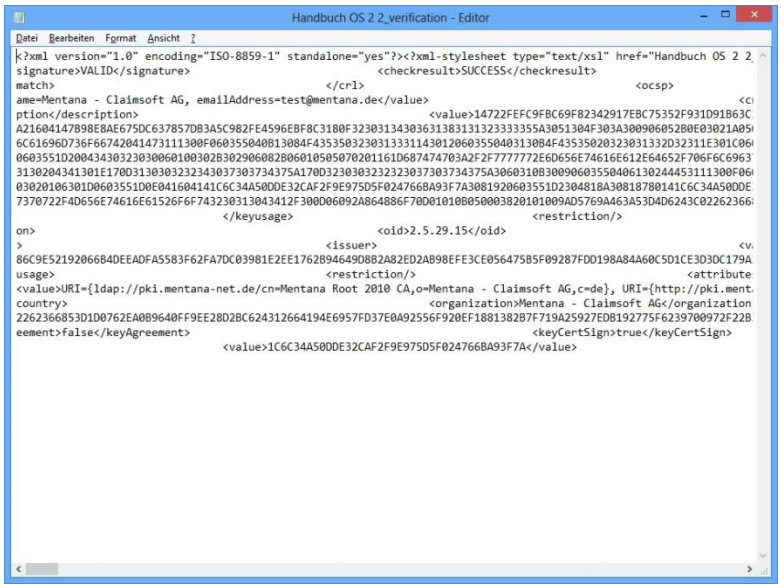

Abbildung 4-37 Verifikations-Protokoll mit fehlendem xslt-Style-Sheet

Falls Sie über keine Internet-Verbindung verfügen, können Sie den Verweis auf die xslt-Datei aus dem Protokoll manuell entfernen. Damit können Sie dann das Ergebnis in „einigermaßen" leserlicher Form betrachten.

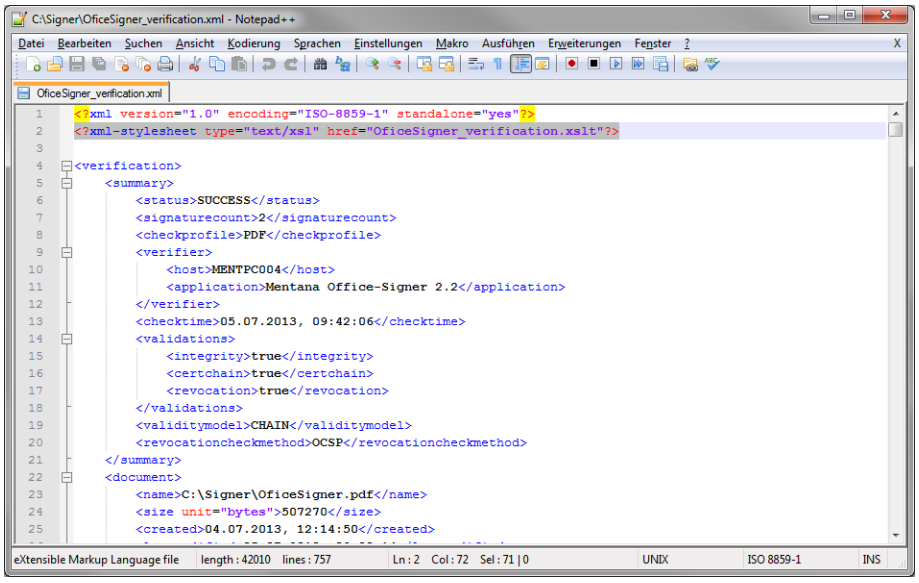

Abbildung 4-38 Manueller Eingriff in das Verifikations-Protokoll

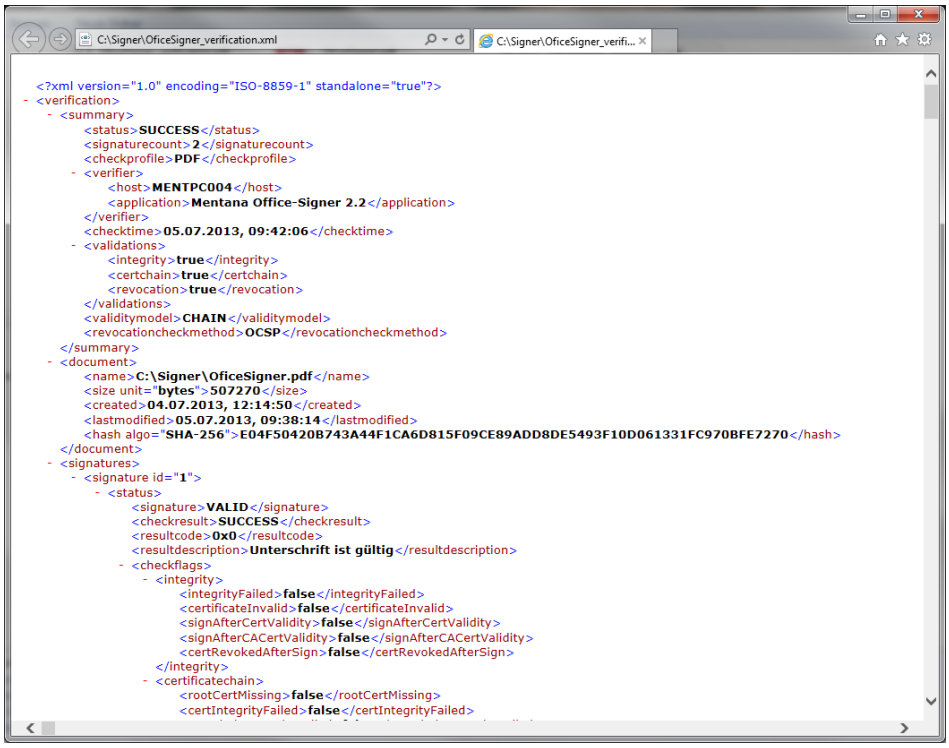

Abbildung 4-39 XML-Anzeige im Internet-Explorer ohne xslt-Verweis

Sollten Sie allerdings eine Internet-Verbindung besitzen, so können Sie die xslt-Datei vom OfficeSigner herunterladen lassen (siehe Kapitel 5.9.2). Ist dies korrekt eingestellt erhalten Sie nach einer Verifikation drei Dateien:

Abbildung 4-40 Anzeige Verzeichnis mit PDF, Verifikationsprotokoll und xslt-Datei

Klicken Sie jetzt auf die XML-Datei, bzw. wählen Sie Öffnen, wird der Internet Explorer gestartet, das korrekte Style-Sheet wird geladen und das Verifikations-Protokoll erscheint wie folgt:

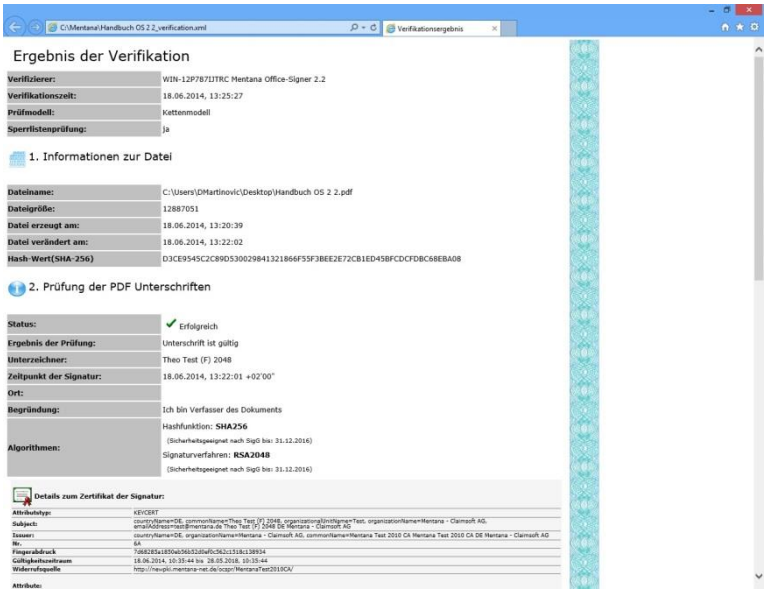

Abbildung 4-41 Verifikationsprotokoll

4.2.2 Überprüfen eingebetteter Signaturen im Adobe Reader

Alternativ zum in Abschnitt 3.2.1 beschriebenen Verfahren, können Sie in PDF-Dokumente eingebettete Unterschriften unter Verwendung des Adobe Readers überprüfen. Öffnen Sie das signierte PDF-Dokument im Adobe Reader und wählen Sie am linken Rand des Programmfensters die Registerkarte Unterschriften aus. Daraufhin zeigt Ihnen der Adobe Reader sämtliche Unterschriften sowie den jeweiligen Überprüfungsstatus an. Hierbei wird der Überprüfungsstatus durch die folgenden Symbole gekennzeichnet:

- **grünes Häkchen:** Die angezeigte Version ist unverändert, das Zertifikat des Unterzeichners ist gültig.
- **grünes Häkchen mit Warnhinweis:** Die eingebettete Unterschrift bezieht sich auf eine vorherige Version des Dokumentes. Die unterschriebene Version und das Zertifikat des Unterzeichners sind vollständig gültig, entsprechen aber nicht der angezeigten Version. Klicken Sie eine derartige Unterschrift an und wählen Sie die Funktion Unterschriebene Version anzeigen um den Zustand des Dokumentes zu sehen, auf den sich die Unterschrift bezieht
- **rotes Kreuz:** Die Unterschrift konnte nicht erfolgreich verifiziert werden. Zugrunde liegende Ursache ist entweder, dass das Dokument verändert wurde oder die Validität des Unterzeichnerzertifikates nicht überprüft werden konnte. Klicken Sie das Unterschriftenfeld an und wählen Sie die Funktion Eigenschaften. um die Ursache angezeigt zu bekommen.
- **graues Fragezeichen:** Die Prüfung der Unterschrift konnte überhaupt nicht durchgeführt werden. Ursache kann ein fehlerhaftes Unterschriftenfeld oder ein nicht unterstützter Verschlüsselungsalgorithmus sein.

! Warnhinweise!

Die Signaturprüfung (Verifikation) in Adobe Reader genügt aus einigen Gründen nicht den Anforderungen des deutschen Umsatzsteuer und Signaturgesetzes (Die Aussage gilt auch für die EU und CH mit Ausnahme von UK und IR).

a) falsche (nicht gesetzlich vorgeschriebene) Prüfmethode. Der Adobe Reader verwendet das sog. "Schalenmodell". Vorgeschrieben ist jedoch das sog. Kettenmodell".

b) keine Unterstützung von SHA-2 Algorithmen die gesetzlich ab 06/2008 verpflichtend sind (Stand 12/2009). Keine Unterstützung von Signaturen auf Basis von eliptischen Kurven (A).

c) keine Protokollierung der Prüfergebnisse gemäß GDPdU/GOBS da der Acrobat- Reader das Prüfergebnis nicht festhält sondern bei jedem öffnen überschreibt.

d) Hohe technische Anforderungen an den Nutzer am Desktop, da für eine erfolgreiche Prüfung im Reader alle Rootzertifikate der potenziellen Versender manuell installiert werden müssten. Das sind per Stand 2008 ca. 200 Zertifikate um für alle Versender eine Prüfung durchführen zu können. Deshalb ist die Onlineprüfung immer der sicherste Weg. Nutzen Sie dazu den kostenlosen Service unter www.signaturportal.de

4.2.3 VERIFIZIEREN EINER EXTERNEN SIGNATUR

Öffnen Sie das Kontext-Menü der externen Signaturdatei und wählen im OfficeSigner-Menü die Funktion Verifizieren (Abbildung 4-42).

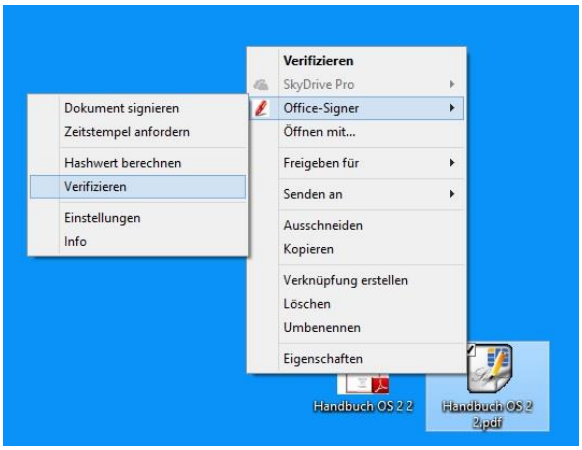

Abbildung 4-42 OfficeSigner-Menü – Verifizieren (Kontextmenü)

Im Verifikationsergebnis-Dialog werden Sie über das Ergebnis der Unterschriftsprüfung informiert (Abbildung 4-43). Sie können das Ergebnis in eine Protokolldatei speichern indem Sie auf Protokoll speichern klicken (Abbildung 4-44).

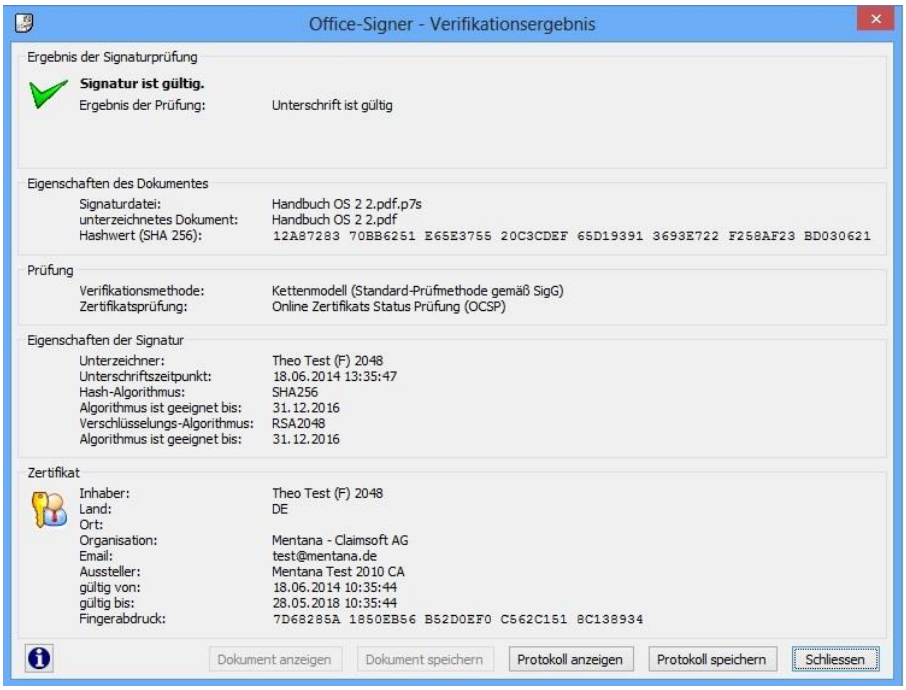

Abbildung 4-43 Verifikationsergebnis

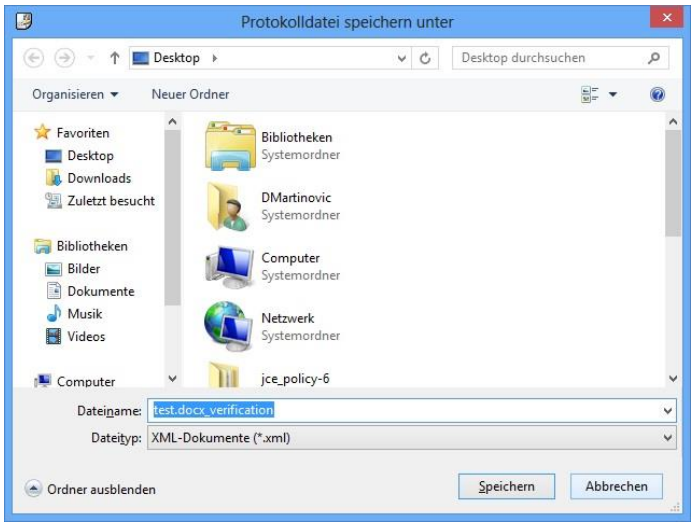

Abbildung 4-44 Dateidialog Protokoll speichern

Das Protokoll der Verifizierung wird in einer XML[10] -Datei gespeichert (Abbildung 4-45).

Abbildung 4-45 Dateiliste mit externer Signatur und Protokolldatei

Öffnen Sie die Protokolldatei, um weitere Informationen über die Verifikation zu erhalten (Abbildung 4-46). Damit das Protokoll richtig angezeigt werden kann, benötigen Sie einen Internetzugang.

[10] XML – Extensible Markup Language. XML ist eine Meta-Sprache, mit der es möglich ist, Auszeichnungssprachen für Dokumente zu erzeugen.

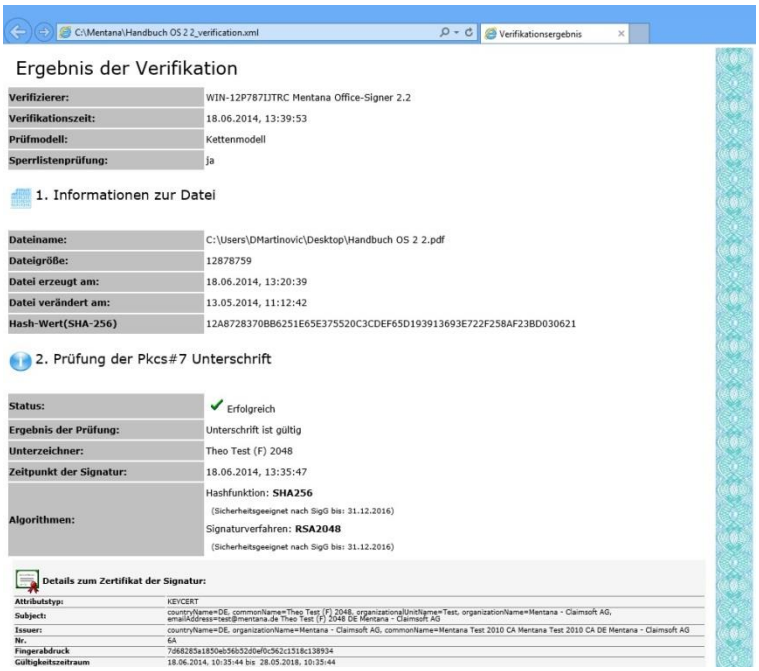

Abbildung 4-46 Verifikationsprotokoll

4.2.4 VERIFIZIEREN EINER DE-MAIL

Öffnen Sie das Kontext-Menü der externen Signaturdatei und wählen im OfficeSigner-Menü die Funktion De-Mail-verifizieren (Abbildung 4-47).

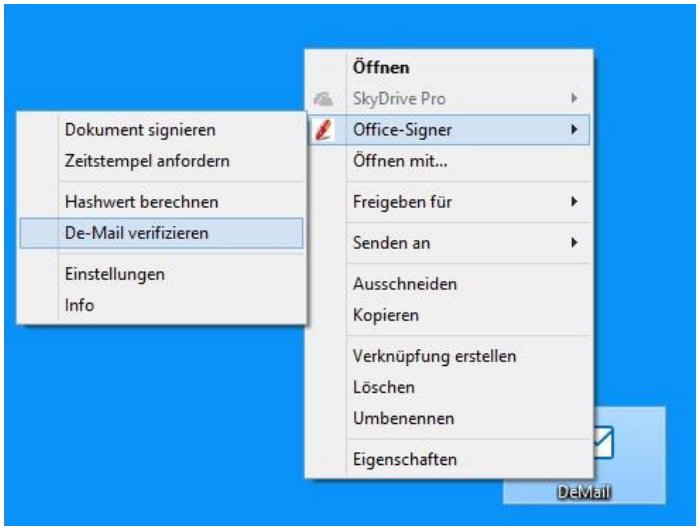

Abbildung 4-47 OfficeSigner-Menü – De-Mail verifizieren (Kontextmenü)

Im Verifikationsergebnis-Dialog werden Sie über das Ergebnis der De-Mail-Prüfung informiert (Abbildung 4-48). Sie können das Ergebnis in eine Protokolldatei speichern indem Sie auf Protokoll speichern klicken (Abbildung 4-49).

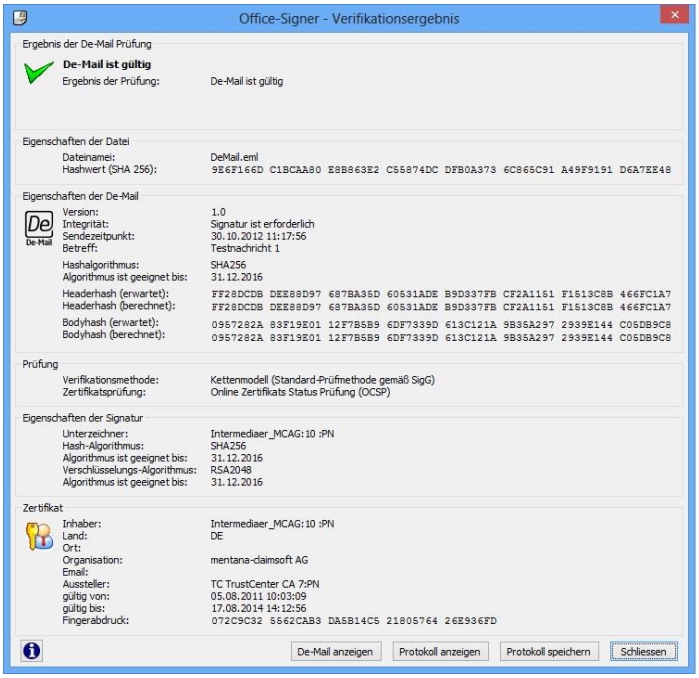

Abbildung 4-48 Verifikationsergebnis De-Mail

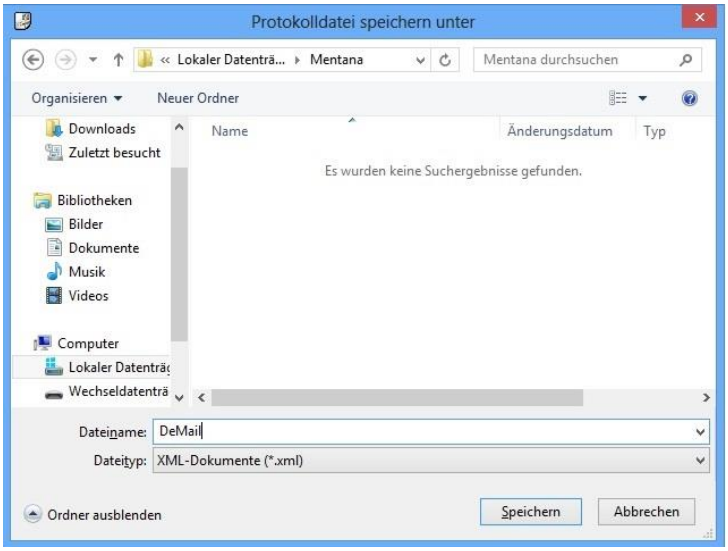

Abbildung 4-49 Dateidialog Protokoll speichern (De-Mail)

Das Protokoll der Verifizierung wird in einer XML[11] -Datei gespeichert (Abbildung 4-50).

Abbildung 4-50 Dateiliste mit De-Mail und Protokolldatei

Öffnen Sie die Protokolldatei, um weitere Informationen über die Verifikation zu erhalten (Abbildung 4-51). Damit das Protokoll richtig angezeigt werden kann, benötigen Sie einen Internetzugang.

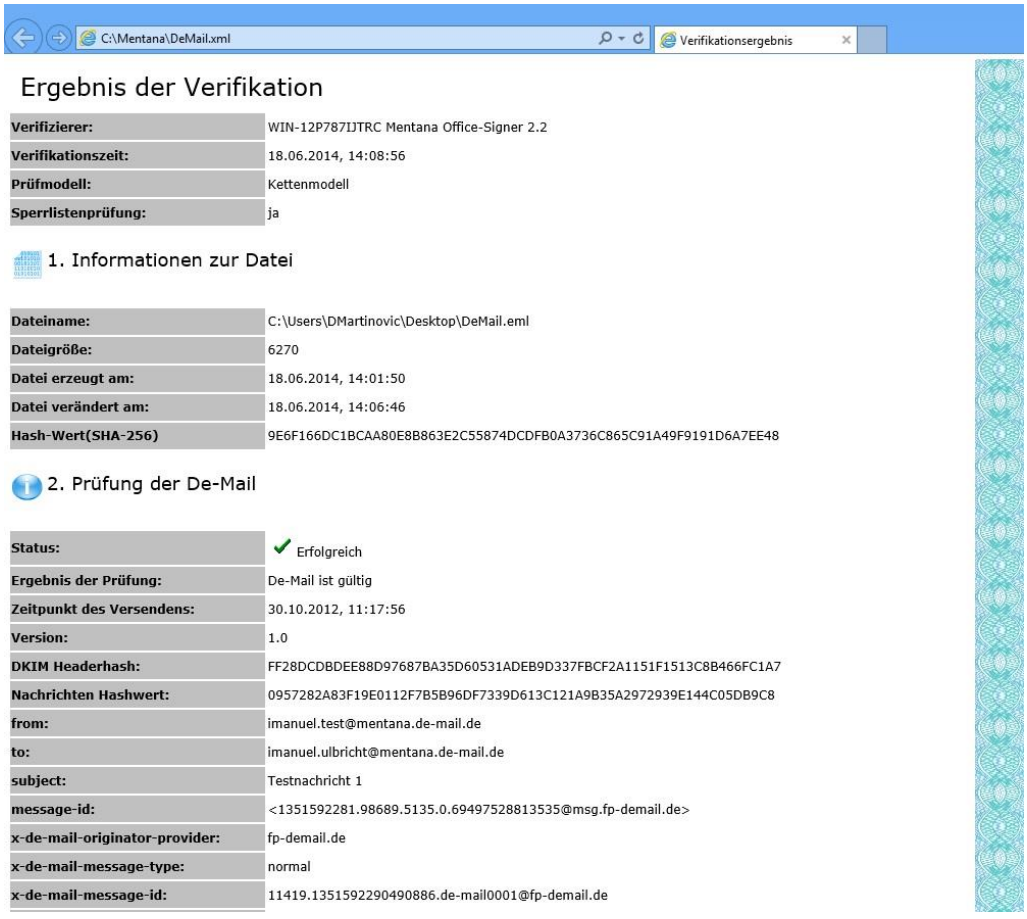

Abbildung 4-51 De-Mail Verifikationsprotokoll

[11] XML – Extensible Markup Language. XML ist eine Meta-Sprache, mit der es möglich ist, Auszeichnungssprachen für Dokumente zu erzeugen.

4.3 ERSTELLEN QUALIFIZIERTER ZEITSTEMPEL

Zeitstempel ermöglichen es Ihnen, den Zustand eines Dokumentes zu einem bestimmten Zeitpunkt nachzuweisen. Sie erhalten hierbei von einem Trustcenter bzw. einen Zeitstempeldienstleister eine Zeitangabe, die untrennbar mit Ihrem Dokument verbunden ist. Der Anbieter garantiert, dass die angegebene Zeit amtlich und verlässlich ist.

Der OfficeSigner unterstützt in der vorliegenden Version den Zeitstempeldienst des Zeitstempel-Anbieters www.signaturportal.de.

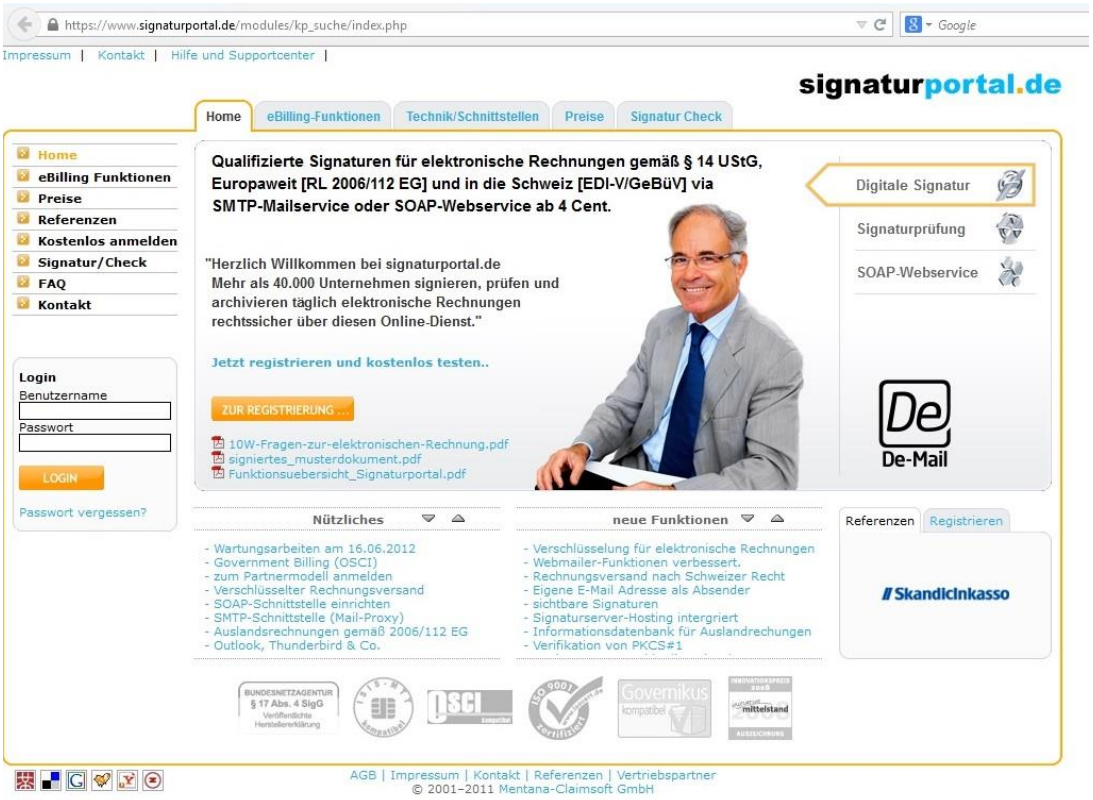

Abbildung 4-52 Startseite Signaturportal

4.3.1 ANMELDUNG BEIM ZEITSTEMPELDIENSTLEISTER

Vor der ersten Verwendung des Zeitstempeldienstes müssen Sie sich beim Betreiber registrieren. Eine genaue Beschreibung zur Konfiguration des Zeitstempeldienstes finden Sie im Abschnitt 4.6.

4.3.2 ANFORDERN EINES ZEITSTEMPELS

Öffnen Sie das Kontext-Menü des Dokumentes, zu dem Sie einen Zeitstempel anfordern wollen und wählen Sie im Menü des OfficeSigner dem Menüpunkt Zeitstempel anfordern aus (Abbildung 4-53). Es öffnet sich eine Meldungsfester mit Informationen zur Anforderung des Zeitstempels (Abbildung 4-54).

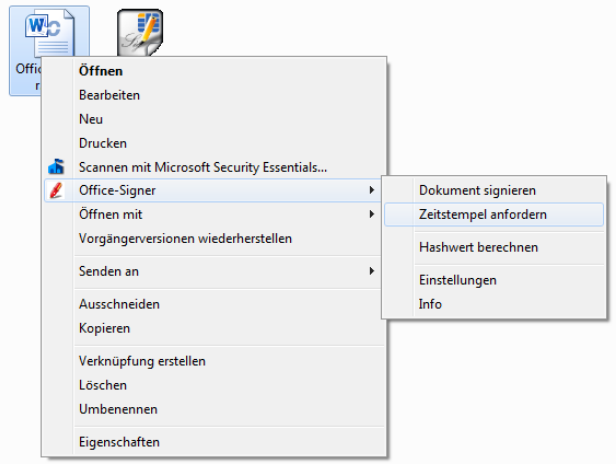

Abbildung 4-53 OfficeSigner-Menü – Zeitstempel (Kontextmenü)

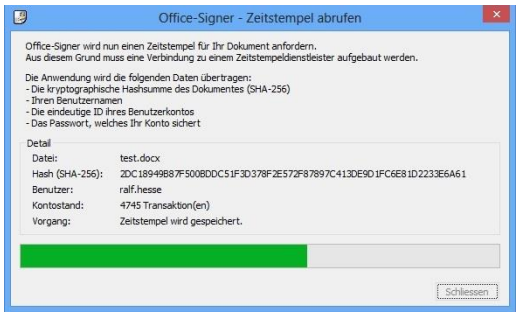

Abbildung 4-54 Verlaufsanzeige Zeitstempelanforderung

Nach erfolgreichem Anfordern des Zeitstempels können Sie alle Informationen noch einmal überprüfen (Abbildung 4-55).

Abbildung 4-55 Zeitstempel erfolgreich angefordert

Der Zeitstempel wird in einer Datei mit dem PKCS7-Format abgelegt. Sie erhält den Namen der Datei, zu der der Zeitstempel angefordert wurde, plus der Erweiterung „.tsr" als Kennzeichnung, dass es sich um einen Zeitstempel handelt (Abbildung 4-56).

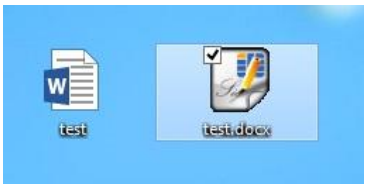

Abbildung 4-56 Dateiliste mit Zeitstempeldatei

Sie können den Zeitstempel auf die gleiche Art und Weise verifizieren wie eine externe Signatur (siehe Abschnitt 3.2.3)

4.4 HASHWERT BESTIMMEN

Hashwerte sind quasi-eindeutige Prüfsummen, die den Zustand eines Dokumentes eindeutig beschreiben. Sie sind darauf ausgelegt, Kollisionen[12] weitestgehend zu vermeiden.

Sie können den OfficeSigner zur Berechnung des Hashwertes beliebiger Dateien verwenden. Öffnen Sie das Kontext-Menü einer Datei und wählen Sie die Funktion Hashwert berechnen aus dem Menü des OfficeSigner. In der sich öffnenden Anzeige (Abbildung 4-57) können Sie sowohl die aktuelle Prüfsumme sehen als auch das zur Berechnung eingesetzte Verfahren (Abbildung 4-58) auswählen.

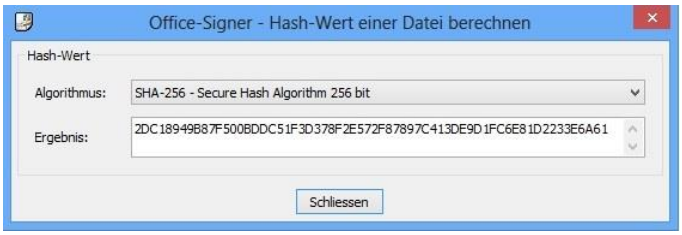

Abbildung 4-57 Hashwert berechnen

[12] Situationen, in denen zwei unterschiedliche Dokumente den selben Hashwert besitzen

Abbildung 4-58 Hashwert Berechnungsverfahren auswählen

Beim Einsatz des OfficeSigner ergeben sich zwei wichtige Anwendungen für die Hashwert-Berechnung

1. Sie können die Hashwerte einsetzen um die Gültigkeit eines archivierten Prüfprotokolls zu verifizieren. Diese enthalten den SHA256-Hash der überprüften Datei. Sind Hashwert- und im Protokoll genannte Prüfsumme identisch, so ist eine erneute Verifikation des Dokumentes nicht notwendig.
2. Sie können die Integrität aller Komponenten des OfficeSigner überprüfen. Lassen Sie die Hashwerte aller Bestandteile berechnen und vergleichen Sie sie mit den unter www.mentana-claimsoft.de angegebenen Vergleichswerten.

4.5 INSTALLIERTE VERSION ANZEIGEN

Verwenden Sie die Funktion Info aus dem Menü des OfficeSigner, um sich Versions-Informationen zur installierten Kopie des OfficeSigner anzeigen zu lassen.

4.6 LIZENZIERUNG

Die Verwendung des OfficeSigner setzt die Existenz eines gültigen Lizenzschlüssels voraus. Diesen erhalten Sie entweder als Bestandteil des gelieferten Softwarepaketes oder auf Anfrage von Mentana-Claimsoft GmbH. Falls Sie zum Zeitpunkt der Installation keine Lizenz-Datei besitzen, kontaktieren Sie bitte info@mentana-claimsoft.de. Sie erhalten daraufhin entweder ihre endgültige Lizenzierung bzw. Evaluationsschlüssel, dessen Gültigkeit auf 30 Tage beschränkt ist[13].

Beim ersten Start der Anwendung werden Sie aufgefordert ihren Lizenzschlüssel zu importieren (siehe Abschnitt 2.2). Wenn Sie zu einem späteren Zeitpunkt die Lizenz ändern möchten, ist das über die Funktion Info aus dem Menü des OfficeSigner möglich. Öffnen Sie dazu das Kontext-Menü eine Datei und wählen Info aus dem Menü des OfficeSigner (Abbildung 4-59).

Die Art des gelieferten Schlüssels hängt vom Status Ihrer Bestellung ab[13]

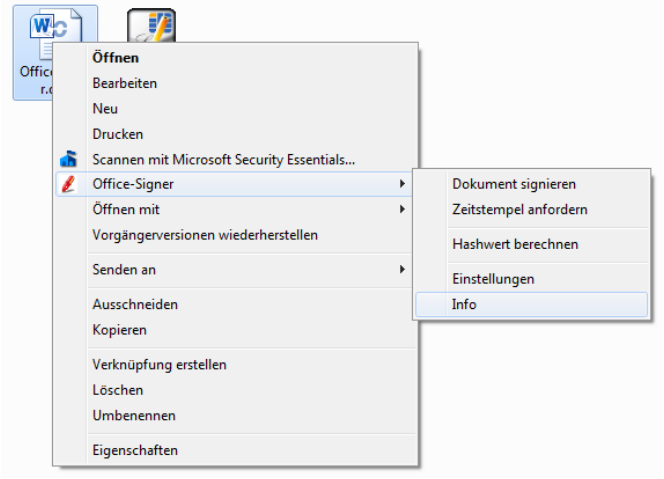

Abbildung 4-59 OfficeSigner-Menü - Info

Im Info-Dialog des OfficeSigner (Abbildung 4-60) können Sie durch Klicken auf Lizenzierung den Lizenzmanager starten (Abbildung 4-61).

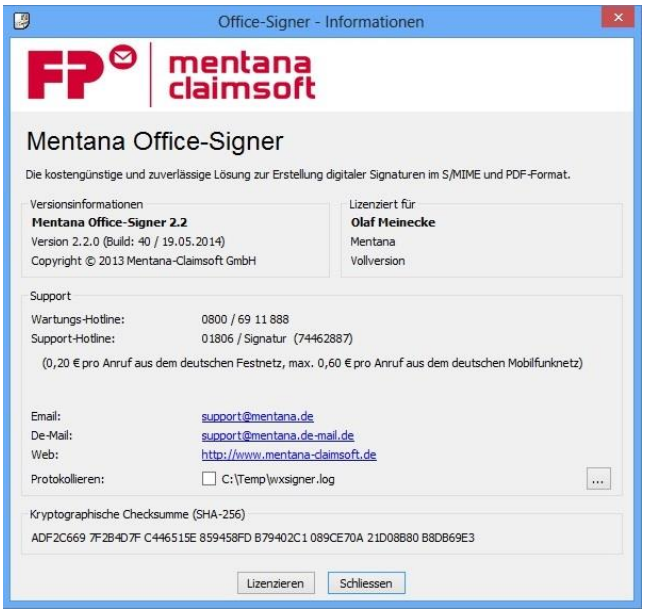

Abbildung 4-60 Info mit Lizenz

Abbildung 4-61 Lizenzmanager ohne Lizenz

Um eine neue Lizenz zu importieren, klicken Sie auf Öffnen und wählen im Öffnen-Dialog die entsprechende Lizenz-Datei aus (Abbildung 4-62).

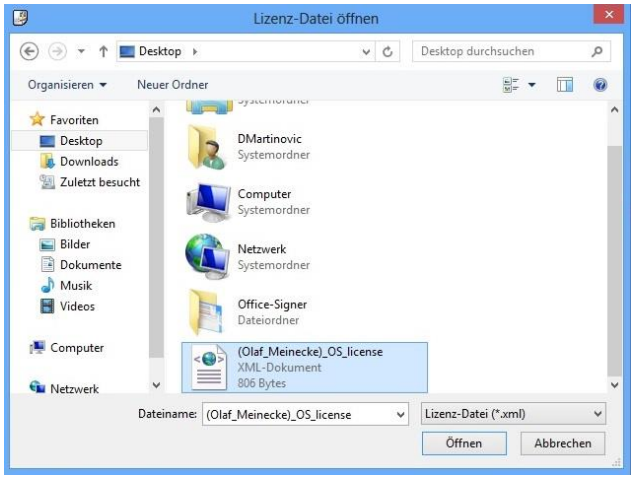

Abbildung 4-62 Lizenz-Datei öffnen

Falls Sie eine gültige Lizenz-Datei geöffnet haben, werden die Lizenzdaten im Lizenzmanager angezeigt und durch einen grünen Balken am unterem Ende des Fensters dargestellt (Abbildung). Mit einem Klick auf Weiter wird die Lizenz importiert. Um zu überprüfen, ob Sie nun die neue Lizenz wirklich importiert haben, rufen Sie erneut die Funktion Info des OfficeSigner wie beschrieben auf und kontrollieren die Lizenzierung (Abbildung 4-63).

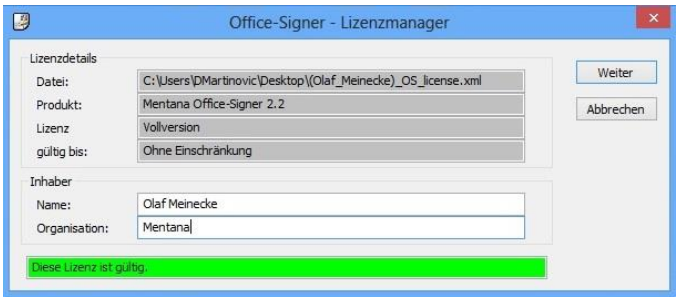

Abbildung 4-63 Lizenzmanager mit gültiger Lizenz

Abbildung 4-64 Info mit gültiger Lizenz

4.7 ANHANG EINFÜGEN (NUR PDF)

Bei PDF-Dokumenten besteht die Möglichkeit beliebige Dateien als Anhang einzufügen. Öffnen Sie das Kontext-Menü der PDF-Datei, in die Sie einen Anhang einfügen wollen und rufen die Funktion Anhang einfügen im OfficeSigner-Menü auf (Abbildung 4-65). Wählen Sie im Öffnen-Dialog (Abbildung 4-66) die Datei aus, die Sie als Anhang in die PDF-Datei einfügen wollen. Nach erfolgreichem Einfügen des Anhanges erhalten Sie eine Bestätigung (Abbildung 4-67).

Öffnen Sie nun das PDF-Dokument mit dem Anhang. Auf der linken Seite befindet sich das Registerblatt Anlagen. Klicken Sie darauf, um die Liste der Anlagen des Dokumentes anzuzeigen

(Abbildung 4-68). Sie können die Anlagen öffnen (Abbildung 4-69) oder in eine Datei speichern. Natürlich können Sie das PDF-Dokument inklusive Anhang signieren.

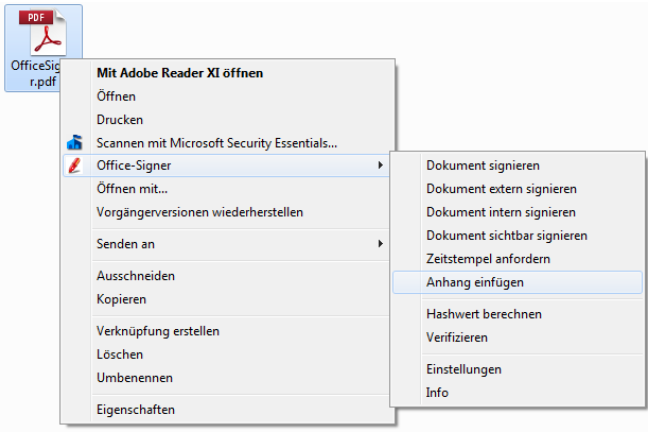

Abbildung 4-65 Anhang einfügen

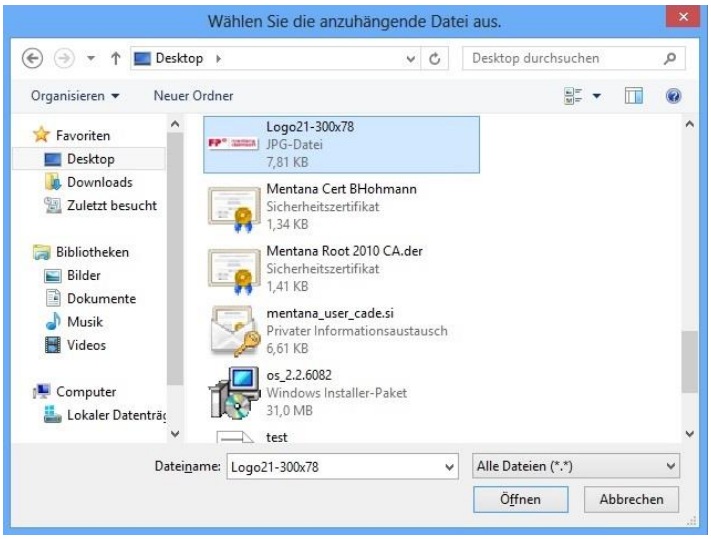

Abbildung 4-66 Anhang auswählen

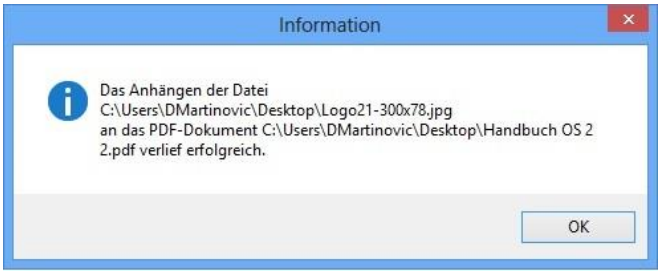

Abbildung 4-67 Bestätigung bei erfolgreich eingefügter Datei

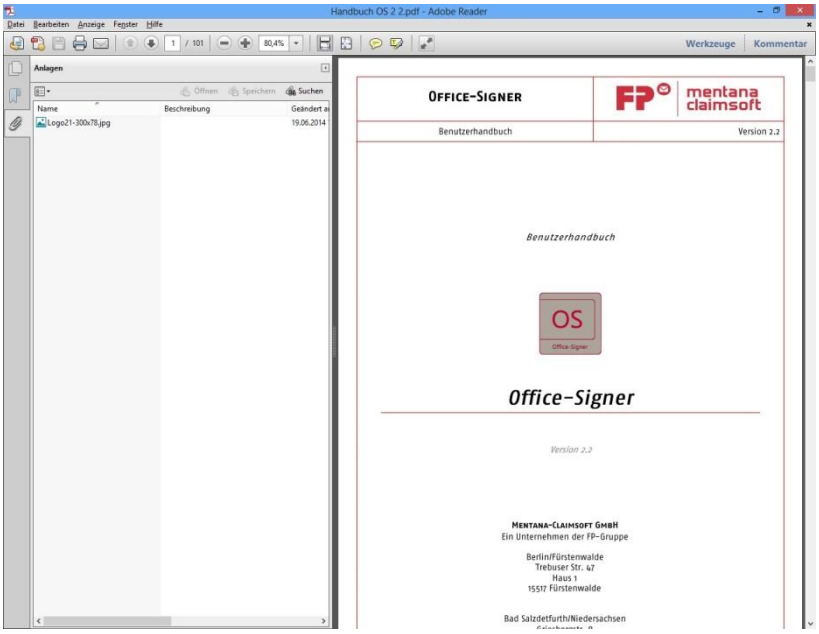

Abbildung 4-68 PDF-Dokument mit Anhang (Adobe Reader)

Abbildung 4-69 geöffneter Anhang des PDF-Dokumentes

4.8 STEUERUNG ÜBER BEFEHLSZEILEN/ PARAMETER

Der OfficeSigner kann auch mit Hilfe von Parametern in der Befehlszeile gesteuert werden.

Beispiele hierfür sind:

- Officesigner.exe /mode=sign /file=c:\daten\test.pdf /posmarkidx=0
- Officesigner.exe /mode=verify /file=c:\daten\test.pdf
- Officesigner.exe /mode=append /file=c:\daten\test.pdf /appendfile=c:\daten\info.dat
- Officesigner.exe /mode=sign /filelist=c:\daten\test.pdf,c:\daten\info.dat
- Officesigner.exe /paramfile=c:\daten\osparams.xml /certserialnum=4474734
- Officesigner.exe /paramfile=c:\daten\osparams.xml /configfile=c:\daten\config.xml

Die Syntax lautet wie folgt:

Officesigner.exe /mode=(mode)

[/file=(file)]

[/filelist=(file1),(file2),..]

[/appendfile=(appendfile)]

[/configfile=(configfile)]

[/posmark=(positionmarker)]

[/posmarkidx=(position index)]

[/outfile=(signed file)]

[/resfile=(result file)]

[/certserialnum=(serialnum)]

[/nogui]

[/setdefcert]

Als Parameter sind möglich:

(mode)

sign – signieren laut Konfiguration und Dateityp

sign_external – extern signieren

sign_internal – intern signieren (nur PDF)

sign_visible – sichtbar signieren (nur PDF)

verify – Verifikation

verify_protocol – Verifikation mit XML-Protokoll (ohne GUI)

append – Datei anhängen (nur PDF)

hash – Hashwert berechnen

timestamp – Zeitstempel anfordern

config – Konfiguration

about – Über Dialog

import_license – Lizenz importieren

enadbg – Debugmod einschalten in c:\temp\signer.log

disdbg – Debugmod ausschalten

usage – Aufrufsyntax anzeigen

(file) – Datei, die signiert, verifiziert, zeitgestempelt, gehasht und an die Dateien angehängt werden sollen.

(filelist) – Liste von Dateien (mit Komma getrennt), die signiert werden

sollen. (z.B.: c:\test.pdf,c:\info.dat,c:\mentana.doc)

(appendfile) – Datei, die angehängt werden soll, wenn /mode=append. (optional)

(configfile) – Konfigurationsdatei für den OfficeSigner. (optional)

(positionmarker) Platzhalterformat zur Festlegung der Position der Unterschrift im Dokument (Vorgabe: „__P@__“ wobei @ durch eine Nummer ersetzt wird: __P1__, __P2__, usw.). (optional)

(posmarkidx) Index des Platzhalters im Dokument. Index 0 bedeutet die nächste freie Position, auf der keine Unterschrift ist. (optional)

(outfile) Signierte Datei (optional)

(resfile) Ergebnis der Signatur in XML-Format (optional)

(certserialnum) Seriennummer des Zertifikates, welches vorausgewählt werden soll (optional)

(nogui) Signatur ohne GUI mit automatischer Zertifikatsauswahl (laut Konfiguration) (optional)

(setdefcert) Setzt das ausgewählte Zertifikat als Standard-Zertifikat (optional)

5 KONFIGURATION DES OFFICESIGNERS

OfficeSigner ist Herstellerseitig für den Betreib nach dem SigG vorkonfiguriert. Besonders ausgebildete und erfahrende Benutzer können nachfolgend beschriebene Abweichende Einstellung vornehmen. Die Funktion Einstellungen aus dem Menü des OfficeSigner erlaubt es Ihnen, Einstellungen für den Betrieb der Anwendung festzulegen.

Öffnen Sie das Kontext-Menü einer beliebigen Datei und wählen Sie die Funktion Einstellungen im OfficeSigner-Menü. Alle Einstellungen werden erst in die Konfiguration übernommen, wenn die die Eingabe mit OK bestätigen.

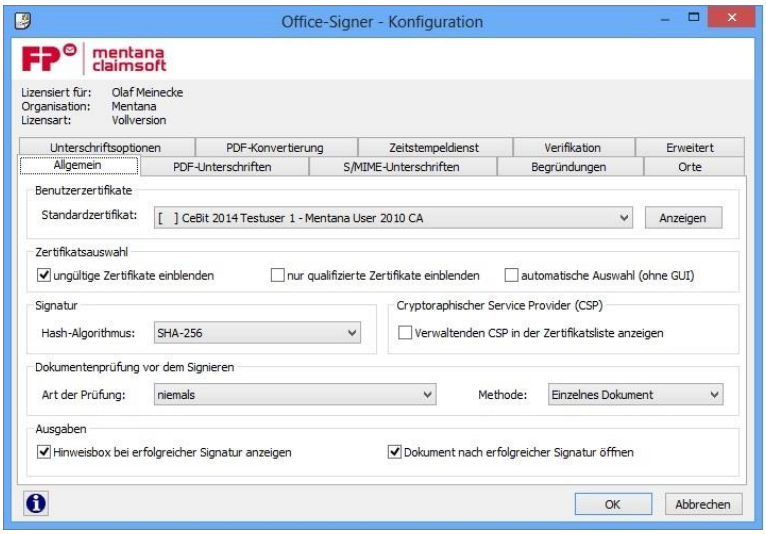

Abbildung 5-1 OfficeSigner Konfiguration

Das Konfigurationsfenster ist wie folgt aufgeteilt: im oberen Bereich sehen Sie Informationen über die aktuell geladene Lizenz. Darunter befindet sich eine Sammlung verschiedenster Karteikarten mit Einstellungsmöglichkeiten. Am unteren Fensterrand befindet sich eine Info-Schaltfläche, sowie eine OK- und eine Abbrechen-Schaltfläche. Mit der OK-Schaltfläche speichern Sie Ihre Änderungen und verlassen die Konfiguration. Die Abbrechen-Schaltfläche verwirft Ihre Eingaben.

Über die Info-Schaltfläche rufen Sie allgemeine Informationen zu Ihrer OfficeSigner-Version auf:

Abbildung 5-2 Infobildschirm OfficeSigner

Die Konfiguration ist aufgeteilt in:

- Allgemein
- PDF-Unterschriften
- S/Mime-Unterschriften
- Begründungen
- Orte
- Unterschriftsoptionen
- PDF-Konvertierung
- Zeitstempeldienst
- Verifikation
- Erweitert

Die jeweiligen Inhalte hängen u.a. ab vom Typ der verwendeten Signatur. Im Folgenden geht dieses Handbuch auf die einzelnen Seiten ein.

5.1 KONFIGURATION ALLGEMEIN

Wählen Sie die Registerkarte Allgemein. Sie können die folgenden Optionen einstellen

- Benutzerzertifikate
- Zertifikatsauswahl
- Signatur
- CSP
- Dokumentenprüfung vor Signatur
- Ausgaben

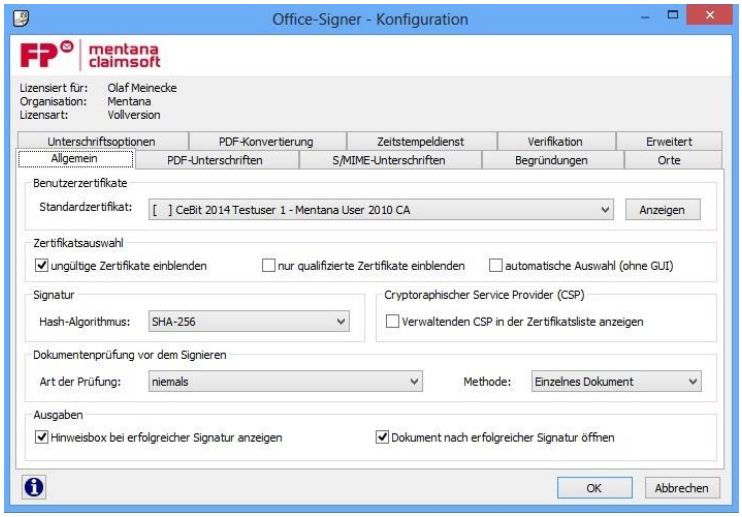

Abbildung 5-3 Seite „Allgemein" der Konfiguration

5.1.1 BENUTZERZERTIFIKATE

Wählen Sie ein Standardzertifikat aus der Liste der verfügbaren Zertifikate aus, das bei jedem Signaturvorgang vorausgewählt sein soll.

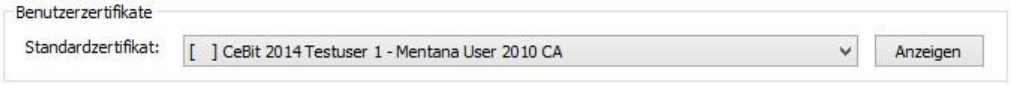

Abbildung 5-4 Konfiguration OfficeSigner allgemein Bereich Benutzerzertifikate

Wenn Sie das Auswahlfeld mit dem auf dem Kopf stehenden Dreieck öffnen, sehen Sie alle verfügbaren Zertifikate (s.u.) zur Auswahl.

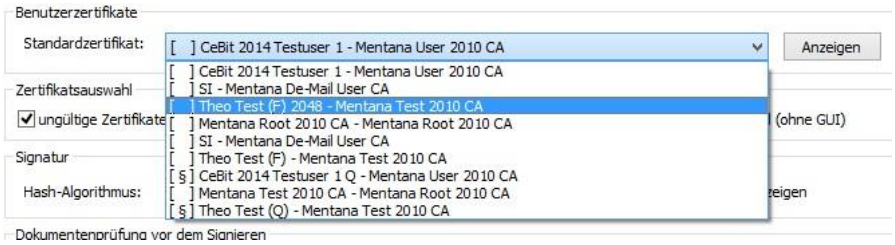

Abbildung 5-5 Geöffnete Zertifikatsliste zur Auswahl

Das Paragraphenzeichen vor dem Zertifikatsnamen gibt an, dass es sich um ein qualifiziertes Zertifikat handelt. Zertifikate ohne das Paragraphenzeichen sind einfache und fortgeschrittene Zertifikate.

Zu jedem ausgewählten Zertifikat kann man sich noch erweiterte Informationen anzeigen lassen, indem man auf die Anzeigen-Schaltfläche klickt.

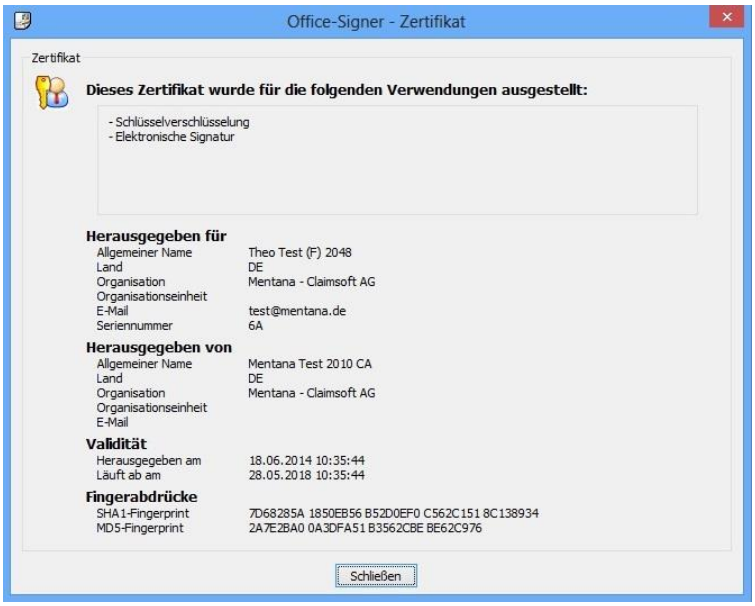

Abbildung 5-6 Weitere Informationen zu einem Zertifikat

5.1.2 ZERTIFIKATSAUSWAHL

Das Auswählen der Option Ungültige Zertifikate einblenden bewirkt, dass bei der Zertifikatsauswahl auch diejenigen Zertifikate angezeigt werden, die nicht für das Erstellen einer elektronischen Signatur verwendbar sind. Abgelaufene Zertifikate, welche noch im Zertifikatsspeicher befinden werden ebenfalls angezeigt, wenn diese Option angeklickt ist.

Wählt man nur qualifizierte Zertifikate einblenden an, so werden in der Auswahlliste nur qualifizierte Zertifikate angezeigt.

Wählt man automatische Auswahl an (ohne GUI), so erfolgt die Auswahl des Zertifikates beim Signieren automatisch. Andernfalls öffnet sich ein Auswahlfenster.

5.1.3 SIGNATUR

Im Bereich Signatur kann man den Hash-Algorithmus auswählen, mit dem signiert wird.

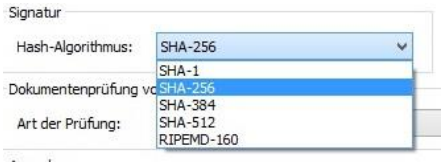

Abbildung 5-7 Auswahl Hash-Algorithmus für Signatur

Hier können Sie zwar alles auswählen, aber nicht alle Algorithmen funktionieren auch mit allen Betriebssystemen. Unter Windows XP muss man zwingen SHA-1 nehmen. Haben Sie eine Signaturkarte, so hängt von dieser ab, welchen Algorithmus Sie auswählen müssen.

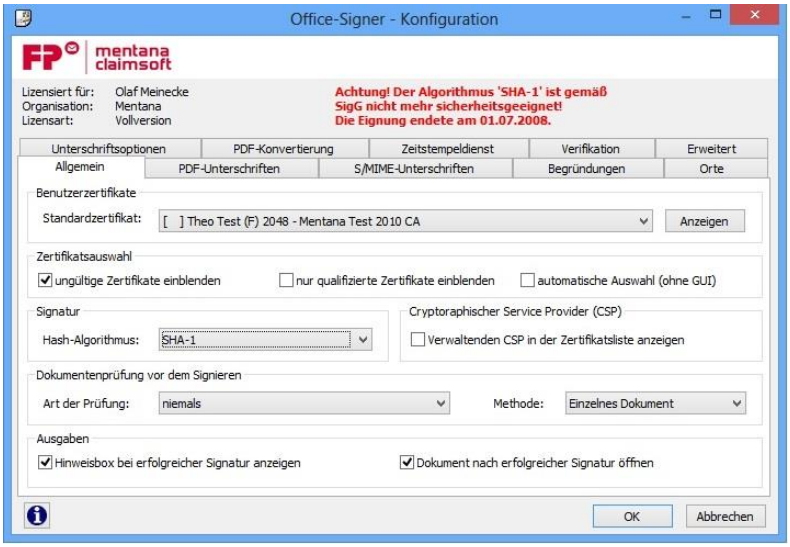

Abbildung 5-8 Meldung bei Wahl vom SHA-1-Algorithmus (veraltet)

5.1.4 CSP

Im Bereich CSP (Cryptographischer Service Provider) können Sie auswählen, ob der CSP in der Liste der Zertifikate für eine Signatur mit angezeigt wird, oder nicht.

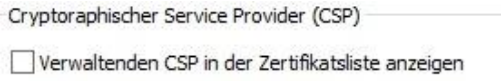

Abbildung 5-9 Auswahl Anzeige CSP in Zertifikatsliste

5.1.5 DOKUMENTENPRÜFUNG VOR SIGNATUR

Vor dem Anbringen einer Signatur kann der OfficeSigner die entsprechenden Dokumente noch einmal für eine optische Prüfung durch den Anwender anzeigen. Hier können Sie auswählen, welche Bedingung hierfür gelten muss:

Abbildung 5-10 Bedingung der Dokumentenprüfung vor einer Signatur

Ist dies angewählt, können Sie die PDF´s noch einmal betrachten, bevor Sie diese signieren. Sollten Sie mehrere PDF´s signieren wollen, können Sie noch die Art der Anzeige wählen.

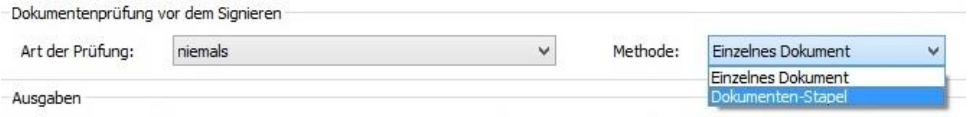

Abbildung 5-11 Prüfungsmethode für Dokumente vor einer Signatur

Mögliche Methoden sind hierbei:

- Einzelnes Dokument: für jedes Dokumente können Sie einzeln „Signieren" wählen
- Dokumenten-Stapel: erst nachdem Sie alle Dokumente betrachtet haben, werden alle signiert.

5.1.6 AUSGABEN

Im Bereich Ausgaben, können Sie die Ausgaben des OfficeSigners nach einer Signatur steuern.

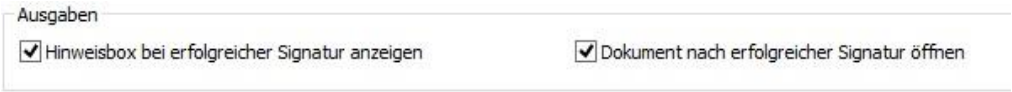

Abbildung 5-12 Konfiguration Allgemein-Ausgaben nach der Signatur

Das Aktivieren der Option Hinweisbox bei erfolgter Signatur anzeigen bewirkt, das Sie nach erfolgreichem Signieren eine Hinweisbox als Bestätigung erhalten.

Wenn Sie ein unterschriebenes PDF-Dokument nach erfolgter Signierung angezeigt haben wollen, dann aktivieren Sie die Option Dokument nach erfolgter Signatur öffnen.

5.2 KONFIGURATION PDF-UNTERSCHRIFTEN

Wählen Sie einen Standard-Unterschriftstyp aus, der bei jedem Signaturvorgang vorausgewählt sein soll.

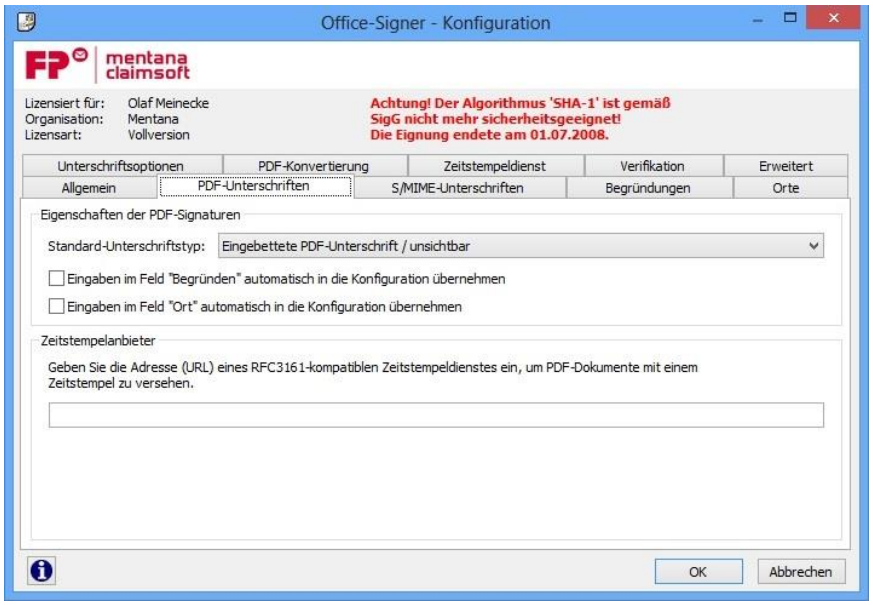

Abbildung 5-13 Konfiguration der PDF-Unterschriften

Falls Sie Eingebettete PDF-Unterschrift ausgewählt haben, doch eine nicht PDF-Datei unterzeichnen wollen, wird gleich die Externe Signatur vorausgewählt.

Das Aktivieren der Option Eingaben im Feld „Begründung“ automatisch in die Konfiguration übernehmen bewirkt, das Eingaben im Feld Begründung, die Sie während einer Signierung vornehmen, automatisch in der Konfiguration abgespeichert werden. Das hat den Vorteil, dass diese neu Begründung beim nächsten Signaturvorgang in der Auswahlliste der Begründungen zur Verfügung steht. Gleiches gilt auch für die Option Eingaben im Feld “Ort“ automatisch in die Konfiguration übernehmen.

In dem Feld Zeitstempelanbieter können Sie die URL eines RFC3161-kompatiblen Zeitstempelanbieters eintragen, über den Sie beim PDF-Signieren auch noch einen Zeitstempel abrufen können.

5.3 KONFIGURATION S/MIME-UNTERSCHRIFTEN

Für eine eventuell durchzuführende S/Mime-Signatur können Sie hier auswählen, ob diese extern oder intern erfolgen soll.

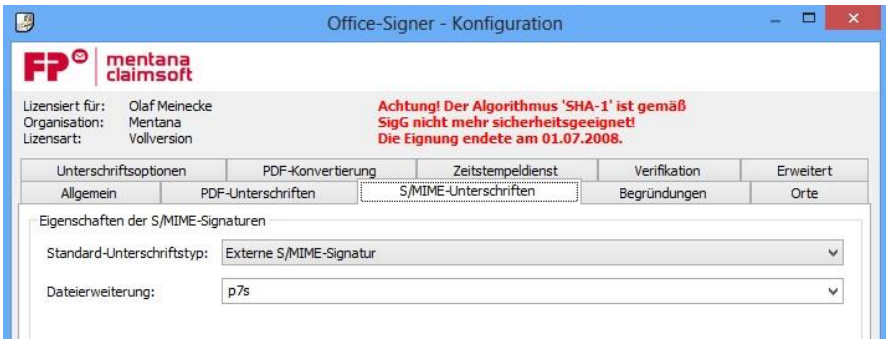

Abbildung 5-14 Konfiguration der S/Mime-Signatur

Bei einer externen Signatur (S/Mime) können Sie eine Dateierweiterung angeben, welche dann vom OfficeSigner benutzt wird.

5.4 KONFIGURATION BEGRÜNDUNGEN

Auf dem Registerblatt Begründungen können Sie Ihre Begründungen verwalten. Folgende Aktionen können durchgeführt werden:

- Begründungen hinzufügen
- Begründungen bearbeiten
- Begründungen löschen
- Eine Begründung als Standard festlegen

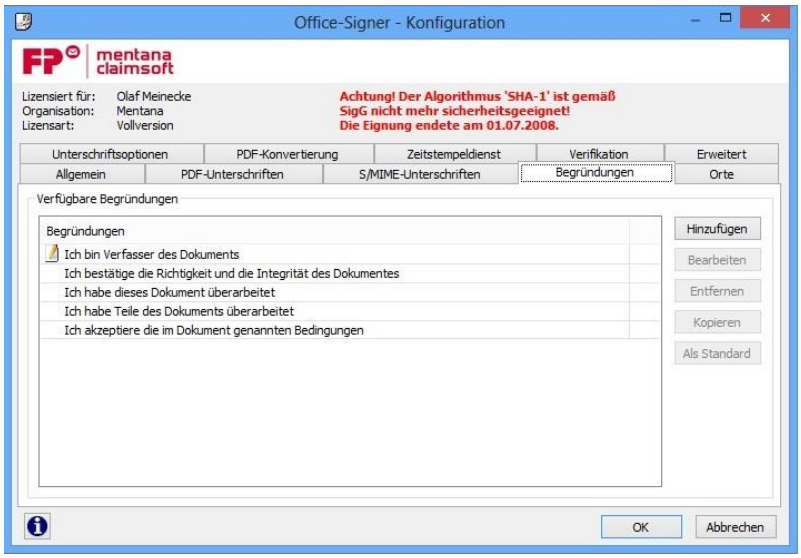

Abbildung 5-15 Konfiguration der Begründungen

5.4.1 HINZUFÜGEN EINER BEGRÜNDUNG

Um eine neue Begründung zu erfassen, klicken Sie auf Hinzufügen (Abbildung 5-15). Im Bearbeiten-Dialog (Abbildung 5-16) erfassen Sie nun die neue Begründung und bestätigen diese mit OK. Nun erscheint die neue Begründung in der Liste.

Abbildung 5-16 Begründung erfassen

5.4.2 BEARBEITEN EINER BEGRÜNDUNG

Um eine Begründung zu bearbeiten, wählen Sie die zu bearbeitende Begründung in der Liste aus und klicken auf Bearbeiten. Im Bearbeiten-Dialog (Abbildung 5-17) können Sie nun die Änderungen vornehmen. Bestätigen Sie Ihre Änderungen mit OK oder verwerfen Sie sie mit Abbrechen.

Abbildung 5-17 Bearbeiten einer Begründung

5.4.3 LÖSCHEN EINER BEGRÜNDUNG

Falls Sie eine Begründung nicht benötigen können Sie diese aus der Liste löschen. Wählen Sie die zu löschende Begründung aus und klicken Sie auf Löschen. Die ausgewählte Begründung wird dann sofort aus der Liste gelöscht.

5.4.4 STANDARD-BEGRÜNDUNG FESTLEGEN

Sie können eine Begründung aus der Liste als Standard definierten. Diese Begründung wird beim Signieren vorausgewählt. Wählen Sie die Begründung aus, die Sie als Standard festlegen wollen und klicken Sie auf Als Standard. Die Standard-Begründung bekommt in der Liste ein kleines Symbol. Es kann immer nur eine Begründung als Standard definiert werden. Falls eine andere Begründung der Standard war, verliert diese die Eigenschaft Standard.

Abbildung 5-18 Als Standard ausgewählte Begründung

5.5 KONFIGURATION ORTE

Auf dem Registerblatt Orte können Sie Ihre Orte verwalten. Folgende Aktionen können durchgeführt werden:

- Ort hinzufügen
- Ort bearbeiten
- Ort löschen
- Einen Ort als Standard festlegen

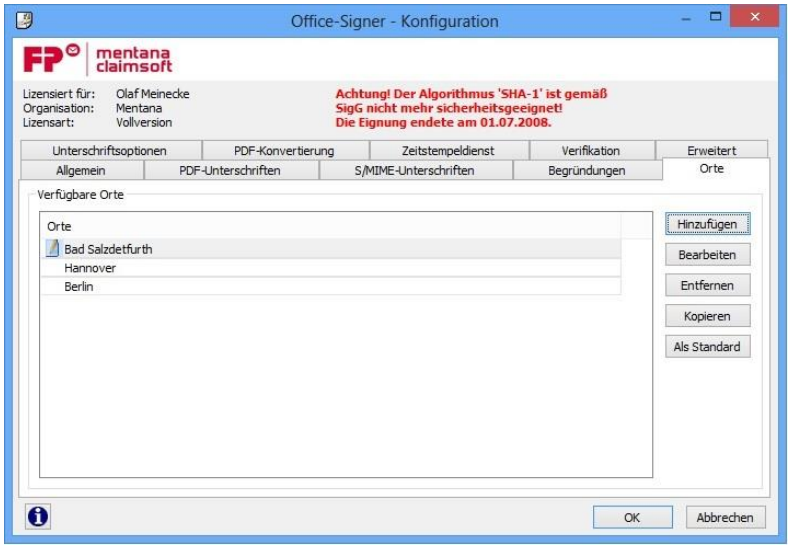

Abbildung 5-19 Konfiguration der Orte

5.5.1 HINZUFÜGEN EINES ORTES

Um einen neuen Ort zu erfassen, klicken Sie auf Hinzufügen. Im Bearbeiten-Dialog erfassen Sie nun den neuen Ort und bestätigen diesen mit OK. Nun erscheint der neue Ort in der Liste.

5.5.2 BEARBEITEN EINES ORTES

Um einen Ort zu bearbeiten, wählen Sie den zu bearbeitenden Ort in der Liste aus und klicken auf Bearbeiten. Im Bearbeiten-Dialog können Sie nun die Änderungen vornehmen. Bestätigen Sie Ihre Änderungen mit OK oder verwerfen Sie diese mit Abbrechen.

5.5.3 LÖSCHEN EINES ORTES

Falls Sie einen Ort nicht benötigen können Sie diesen aus der Liste löschen. Wählen Sie den zu löschenden Ort aus und klicken Sie auf Löschen. Der ausgewählte Ort wird dann sofort aus der Liste gelöscht.

5.5.4 STANDARD-ORT FESTLEGEN

Sie können einen Ort aus der Liste als Standard definierten. Dieser Ort wird beim Signieren vorausgewählt. Wählen Sie den Ort aus, den Sie als Standard festlegen wollen und klicken Sie auf Als Standard. Der Standard-Ort bekommt in der Liste ein kleines Symbol. Es kann immer nur ein Ort als Standard definiert werden. Falls ein anderer Ort der Standard war, verliert dieser die Eigenschaft Standard.

5.6 KONFIGURATION UNTERSCHRIFTSPOSITIONEN

Auf dem Registerblatt Unterschriftspositionen können Sie Ihre Positionen der Unterschriften verwalten. Unterschriftspositionen legen fest, an welcher Stelle des PDF-Dokumentes sich die sichtbare Unterschrift befinden soll. Dabei kann festgelegt werden, dass sich die Unterschrift immer auf einer bestimmten Seite oder auf der letzten Seite des Dokumentes befindet. Die Positionierung der Unterschrift auf der Seite ist relativ oder absolut möglich. Auch kann ein Bild an die Position der Unterschrift eingefügt werden. Ein solches Bild kann zum Beispiel Ihre eingescannte Unterschrift sein.

Folgende Aktionen können durchgeführt werden:

- Unterschriftsposition hinzufügen
- Unterschriftsposition bearbeiten
- Unterschriftsposition löschen
- Eine Unterschriftsposition als Standard festlegen

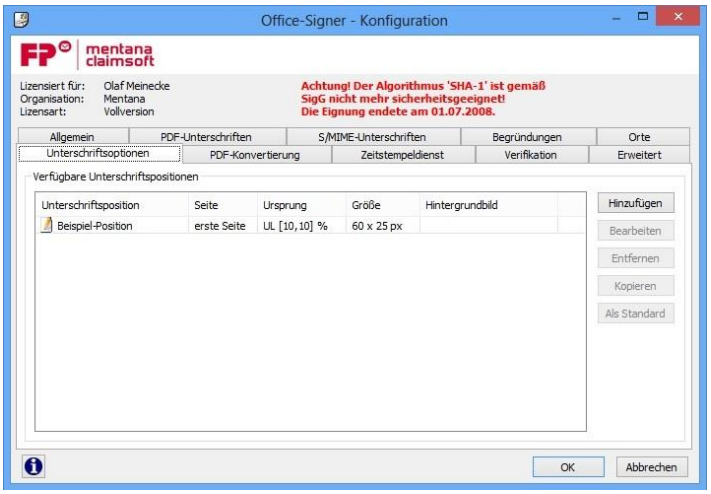

Abbildung 5-20 Konfiguration der Unterschriftspositionen

5.6.1 HINZUFÜGEN EINER UNTERSCHRIFTSPOSITION

Um eine neue Unterschriftsposition anzulegen, klicken Sie auf Hinzufügen (Abbildung 5-20). Der Unterschriftspositionen-Dialog erscheint (Abbildung 5-21).

Abbildung 5-21 Hinzufügen einer Unterschriftsposition

Vergeben Sie einen eindeutigen Namen (Bezeichnung) für die Unterschriftsposition, damit Sie beim Signieren keine Probleme beim Auswählen der richtigen Unterschriftsposition bekommen. Im Feld Position bezogen auf können Sie festlegen an welcher Position auf der Seite sich die Unterschrift befinden soll. Dabei gibt es folgende Möglichkeiten:

- **relative zu links unten (Angaben in Prozent):** Position relative zur unteren linken Ecke der Seite in Prozent. Dabei Zählt die Breite und die Höhe der Seite als 100 %. Bei einer Seitenbreite von 580 Punkten (Pixel) wären 10 % 58 Punkte von der linken Seite. Bei einer Seitenhöhe von 840 Punkten wären 10 % 84 Punkte vom unteren Rand.
- **unten links (Angaben in Pixel):** Position absolut zur linken unteren Ecke der Seite in Punkten (Pixel).
- **oben links (Angaben in Pixel):** Position absolut zur linken oberen Ecke der Seite in Punkten (Pixel).
- **unten rechts (Angaben in Pixel):** Position absolut zur rechten unteren Ecke der Seite in Punkten (Pixel).
- **oben rechts (Angaben in Pixel):** Position absolut zur rechten unteren Ecke der Seite in Punkten (Pixel).

Um die Größe einer Seite eines PDF-Dokumentes zu ermitteln, öffnen Sie das Dokument und rufen im Menü Datei den Menüpunkt Dokumenteigenschaften auf. Im Dokumenteigenschafts-Dialog wählen Sie das Registerblatt Beschreibung und in der Rubrik Erweitert können Sie das Papierformat sehen. Falls Sie das Papierformat nicht in Punkten (Pkt.) angezeigt bekommen. Müssen Sie erst noch die Einheit umstellen. Dazu schließen Sie den Dialog und rufen im Menü Bearbeiten den Menüpunkt Grundeinstellungen auf. Im Grundeinstellungs-Dialog wählen Sie die Kategorie Einheiten und stellen Seiteneinheiten auf `Punkte`. Nun rufen Sie erneut die Dokumenteigenschaften auf und suchen das Papierformat.

Nachdem Sie die Art der Position der Unterschrift auf der Seite festgelegt haben, müssen Sie nun noch festlegen auf welcher Seite sich die sichtbare Unterschrift befinden soll. Dazu wählen Sie im Feld Seite eine der folgenden Möglichkeiten aus:

- **Erste Seite:** Die Unterschrift wird auf die erste Seite positioniert
- **Letzte Seite:** Die Unterschrift wird auf der letzten Seite positioniert
- **Auf Seite:** Die Unterschrift wird auf der von Ihnen festgelegten Seite positioniert.

Die Felder X-Position und Y-Position dienen zum Festlegen der Position auf der Seite in Abhängigkeit von dem Feld Position bezogen auf. Bei einer relativen Positionierung müssen Sie die Angaben in Prozent und bei einer absoluten Positionierung in Punkten hinterlegen. Dabei ist X die horizontale und Y die vertikale Achse (Abbildung 5-22 bis Abbildung 5-25).

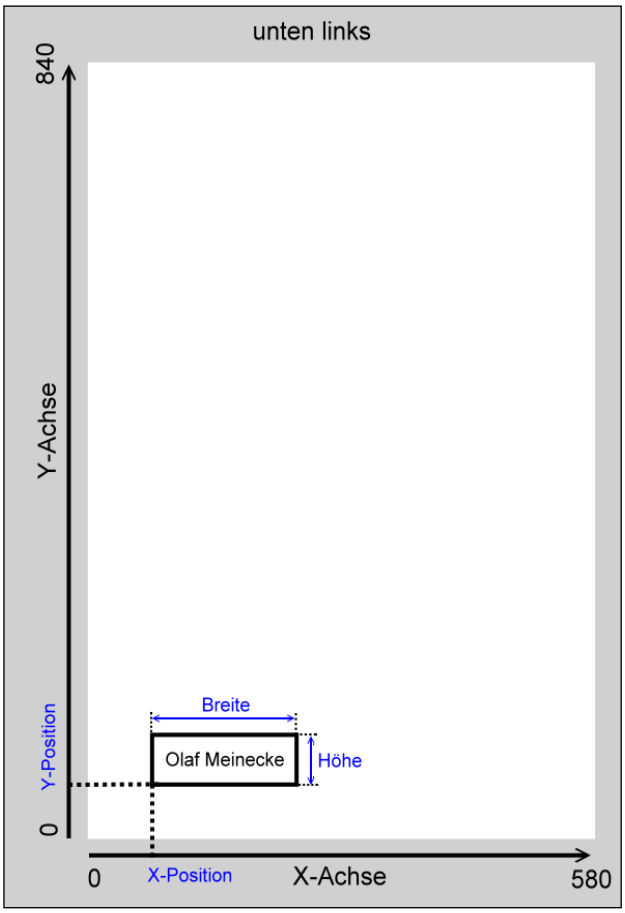

Abbildung 5-22 Werte der Unterschriftsposition bei Positionierung unten links

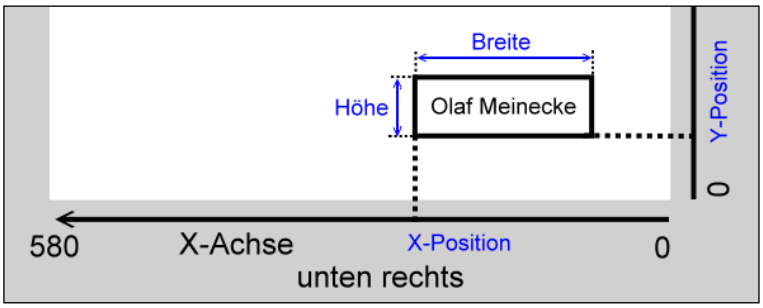

Abbildung 5-23 Werte der Unterschriftsposition bei Positionierung unten rechts

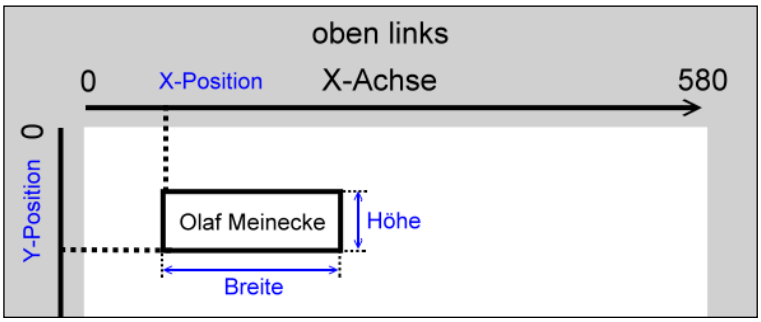

Abbildung 5-24 Werte der Unterschriftsposition bei Positionierung oben links

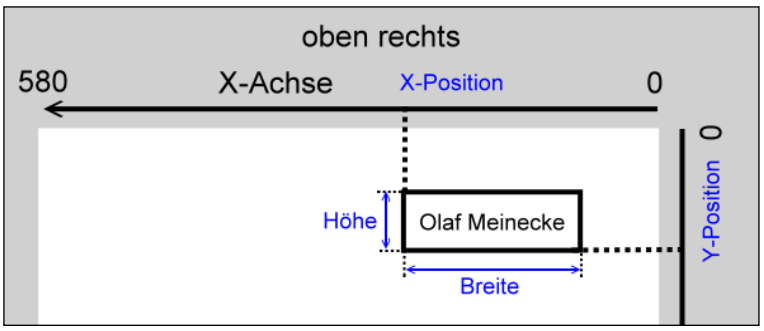

Abbildung 5-25 Werte der Unterschriftsposition bei Positionierung oben rechts

Als nächstes muss der Typ der Unterschrift festgelegt werden. Sie haben die Auswahl zwischen:

- **Unterschriftsfeld:** Normale sichtbare Unterschrift
- **Unterschriftsfeld mit Hintergrundbild:** Sichtbare Unterschrift mit Bild (z.B.: eingescannte Unterschrift)
- Logo mit Unterschriftsfeldern (siehe Kap. 5.6.5)

Wenn Sie Unterschriftsfeld mit Hintergrundbild ausgewählt haben, müssen Sie eine Bilddatei als Hintergrundbild öffnen (Abbildung 5-27). Es können nur Dateien im JPEG-Format als Hintergrund verwendet werden.

In den Feldern Breite und Höhe geben Sie die Breite und die Höhe der sichtbaren Unterschrift ein (Abbildung Abbildung 5-26 Bearbeiten einer Unterschriftsposition). Der Null-Punkt der Box der sichtbaren Unterschrift ist immer unten links.

Abbildung 5-26 Bearbeiten einer Unterschriftsposition

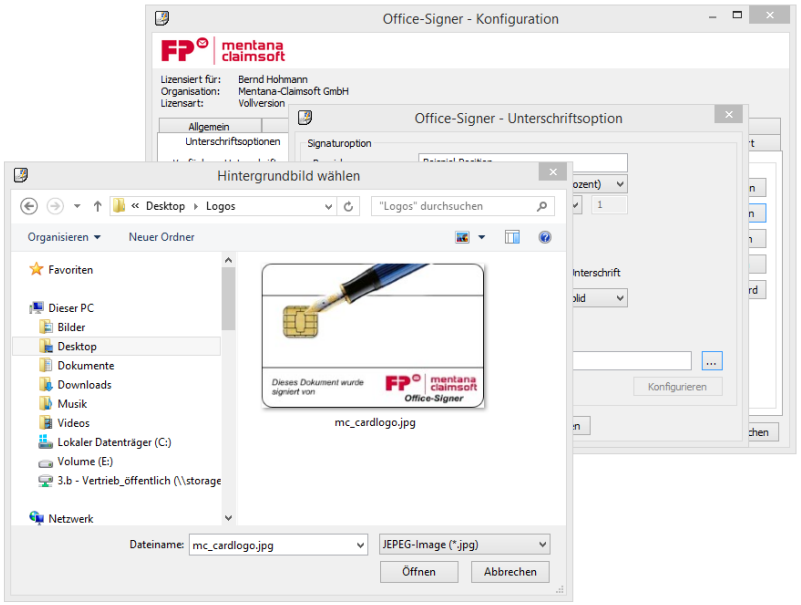

Abbildung 5-27 Hintergrundbild öffnen

Bestätigen Sie Ihre Änderungen mit OK. Die neue Unterschriftsposition erscheint in der Unterschriftspositionen Liste.

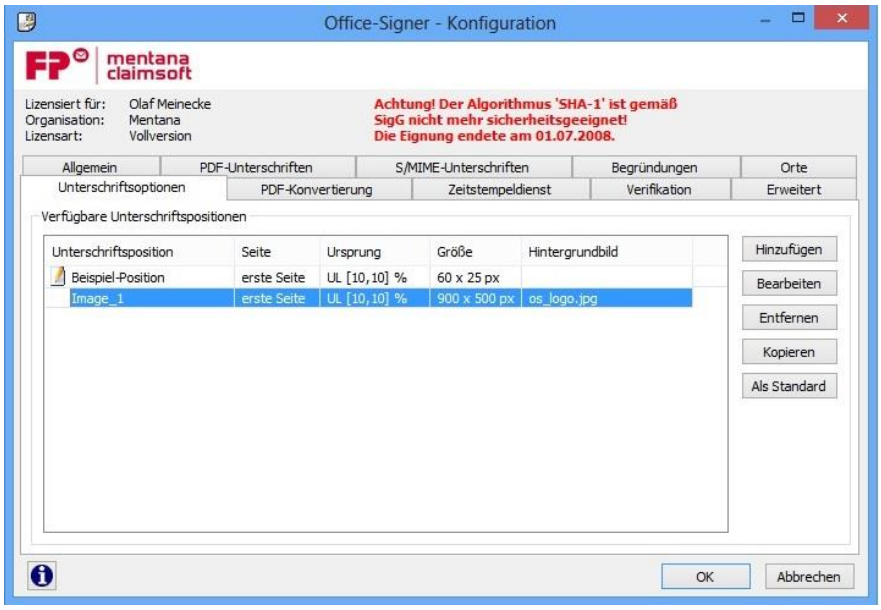

Abbildung 5-28 Liste der Unterschriftspositionen

5.6.2 Bearbeiten einer Unterschriftsposition

Um eine Unterschriftsposition zu bearbeiten, wählen Sie den zu bearbeitenden Eintrag in der Liste aus und klicken auf Bearbeiten. Im Bearbeiten-Dialog können Sie nun die Änderungen vornehmen. Bestätigen Sie Ihre Änderungen mit OK oder verwerfen Sie sie mit Abbrechen.

5.6.3 Löschen einer Unterschriftsposition

Falls Sie eine Unterschriftsposition nicht mehr benötigen können Sie diesen aus der Liste löschen. Wählen Sie den zu löschenden Eintrag aus und klicken Sie auf Löschen. Die ausgewählte Unterschriftsposition wird dann sofort aus der Liste gelöscht.

5.6.4 Standard-Unterschriftsposition festlegen

Sie können eine Unterschriftsposition aus der Liste als Standard definierten. Diese Unterschriftsposition wird beim Signieren vorausgewählt. Wählen Sie den Eintrag aus, den Sie als Standard festlegen wollen und klicken Sie auf Als Standard. Die Standard-Unterschriftsposition bekommt in der Liste ein kleines Symbol. Es kann immer nur ein Eintrag als Standard definiert werden. Falls ein anderer Eintrag der Standard war, verliert dieser die Eigenschaft Standard.

5.6.5 LOGO MIT UNTERSCHRIFTSFELDERN

Weitere Einstellungsmöglichkeiten eines Unterschriftsfeldes haben Sie an dieser Stelle. Wählen Sie Logo mit Unterschriftsfeldern, können Sie das Logo definieren. Anschließend können Sie die jeweils anzuzeigenden Felder in der Unterschrift definieren. Diese Angaben werden in einer XML-Datei gespeichert und können somit immer wieder benutzt werden.

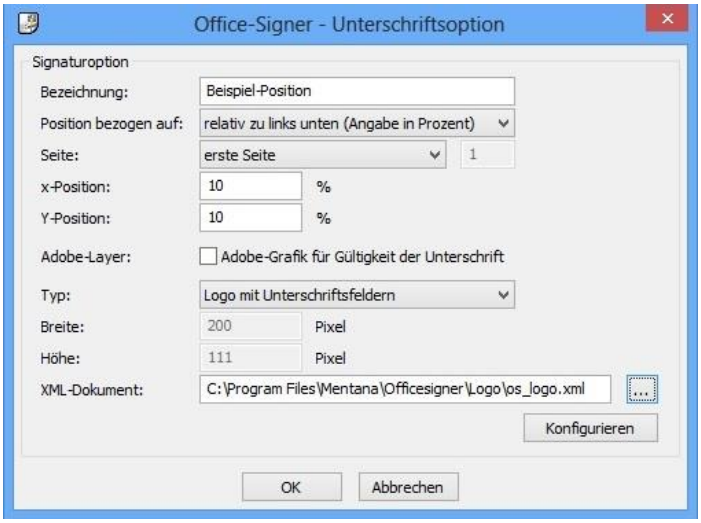

Abbildung 5-29 Unterschriftsoptionen

Nachdem Sie den entsprechenden Typ ausgewählt haben, können Sie den Pfad zu einer XML-Datei angeben. Wenn das Feld noch keinen Dateinamen enthält, so können Sie über den Button Erstellen eine neue Datei erzeugen. Haben Sie schon eine XML-Datei ausgewählt, lautet der Button Konfigurieren.

Mit der Schaltfläche Erstellen gelangen Sie zu einem Fenster für das Aussuchen eins XML-Dateinamens. Wurde ein Dateiname vergeben, so gelangen Sie zum Eingabefenster für die Konfiguration des Logos mit seinen Textfeldern:

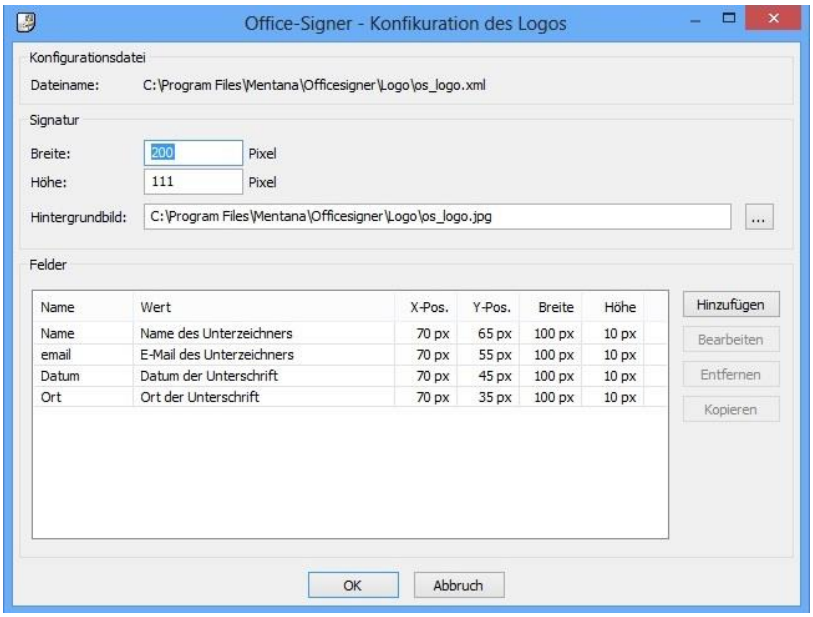

Abbildung 5-30 Logo-Konfiguration

Als erstes können Sie hier bestimmen, welche Grafik im Hintergrund des Unterschriftfeldes angezeigt wird. Dazu können Sie Höhe und Breite des Feldes angeben.

Abbildung 5-31 Hintergrund-Grafik

Die Hintergrund-Grafik muss als JPG vorliegen. Sie wird auf die Breite und Höhe der Signatur angepasst. Bei nicht passenden Seitenverhältnissen wird sie allerdings verzerrt.

Über der Hintergrund-Grafik können einzelne Textfelder angezeigt werden. Die Liste der Textfelder sehen Sie im unteren Fensterbereich:

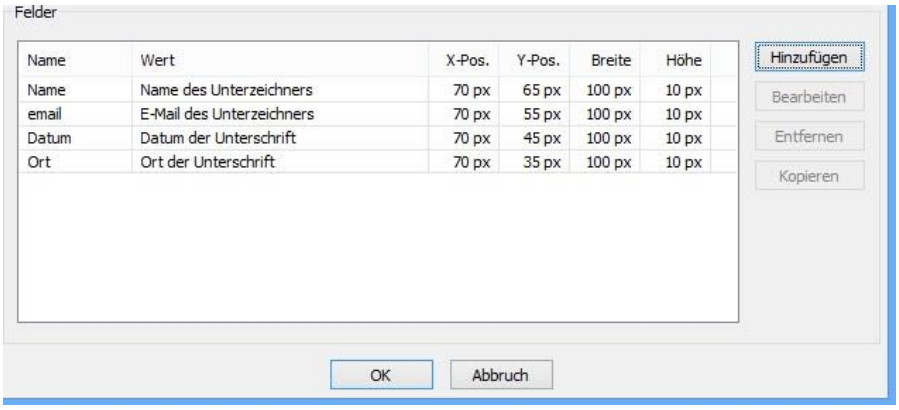

Abbildung 5-32 Feldliste

Über die Schaltfläche Hinzufügen erstellen Sie neue Textfelder. Sie gelangen zum Eingabefenster für die Eigenschaften eines Textfeldes:

Abbildung 5-33 Eigenschaften eines Signaturfeldes

Sie können einen Feldnamen vergeben. Als nächstes müssen Sie auswählen, was in dem Textfeld angezeigt werden soll. Hier können Sie wählen, ob es ein konstanter Text sein soll, den Sie vorgeben, oder ob es einer der Systemtexte (z.B. Datum der Unterschrift) sein soll.

Abbildung 5-34 Liste der Feldwerte

Falls Sie den Eintrag Konstanter Text auswählen, ist das Feld Feldtext aktiviert und Sie können den Wunschtext dort eintragen. Anderfalls ist es deaktiviert.

Als nächstes können Sie eingeben a) an welcher Position innerhalb des Unterschriftsfeldes dies Textfeld erstellt werden soll, sowie b) die Breite und die Höhe. Diese Angaben sind in Pixel einzutragen.

Als weitere Einstellungen können Sie noch das Erscheinungsbild der Schrift beeinflussen:

- Schriftart (Helvetica, TimesNewRoman, Courier)
- Schriftstil (Normal, Fett, Kursiv, Fett&Kursiv)
- Größe
- Ausrichtung (Links, Rechts, Zentriert)

-
- Durch Anwählen von OK werden die Einstellungen übernommen und erscheinen in der Feldliste.

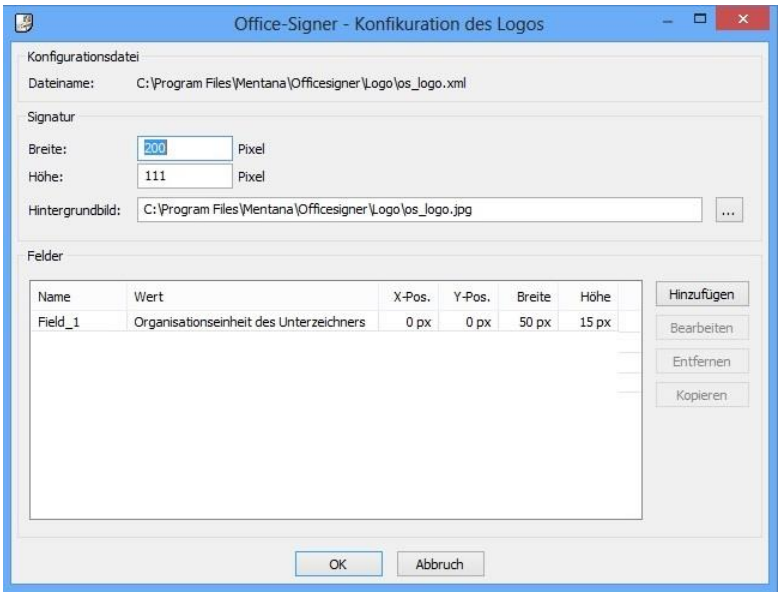

Abbildung 5-35 Feldliste mit einem Eintrag

Im Hintergrund werden die Einstellungen im ausgewählten XML eingetragen:

```
<?xml version="1.0" encoding="ISO-8859-1" standalone="yes"?>
<signatureappearance width="100" height="50">
   <background>C:\Users\Hohmann\Desktop\status_hg.jpg</background>
   <field id="Field_1" content="CERT:OU" width="50" height="15" x="0" y="0"/>
</signatureappearance>
```

5.6.6 LOGOKONFIGURATION PER XML

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.

Ein Beispiel der Konfigurationsdatei sieht wie folgt aus:

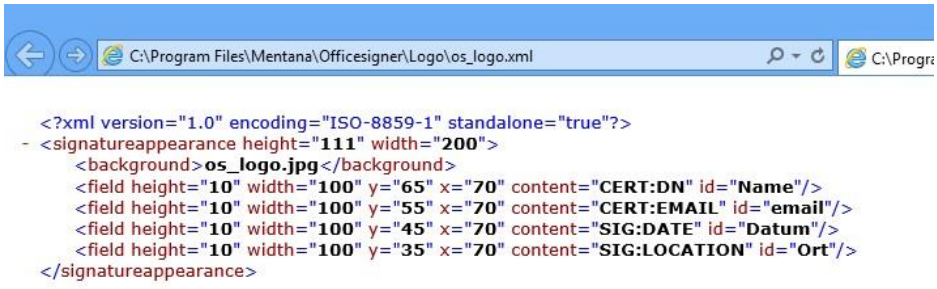

Abbildung 5-36 Beispiel einer XML-Datei

Die Elemente im Einzelnen:

<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.

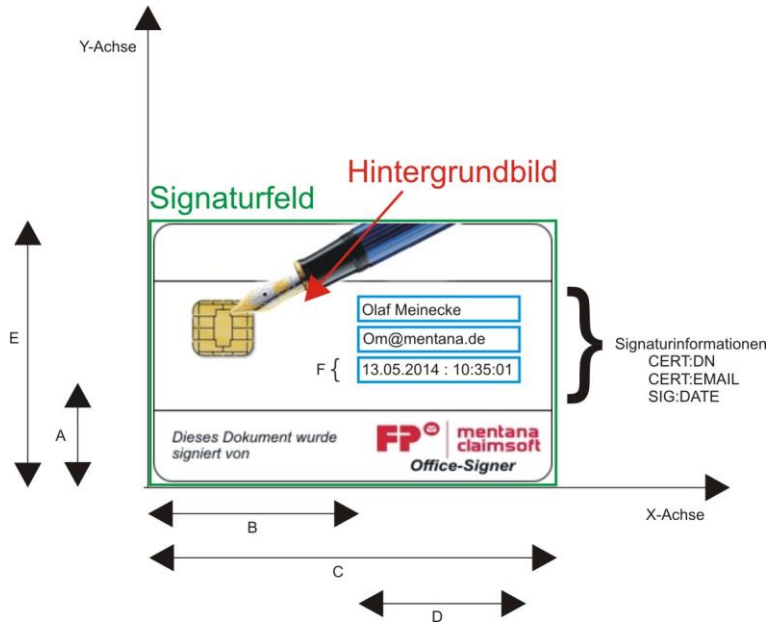

Abbildung 5-37 Bemaßung Signatur- und Textfelder

E: Höhe des Signaturbereichs (grün markiert)

C: Breite des Signaturbereichs (grün markiert)

Einstellungen für ein Textfeld. Hier am Beispiel SIG:DATE (Datum und Uhrzeit der Signatur)

A: Y-Position der linken hinten Ecke des Textfeldes

B: X-Position der linken unteren Ecke des Textfeldes

F: Höhe des Textfeldes

D. Breite des Textfeldes

Alle Angaben sind in Pixel und beziehen sich auf die untere links Ecke des Signaturfeldes.

5.7 KONFIGURATION PDF-KONVERTIERUNG

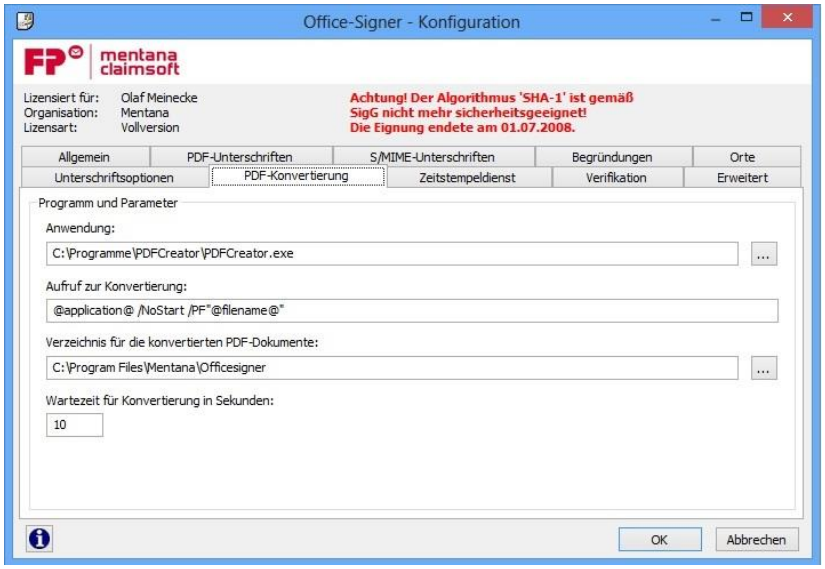

Abbildung 5-38 PDF-Konvertierung

5.8 KONFIGURATION ZEITSTEMPELDIENST

Vor der ersten Verwendung des Zeitstempeldienstes müssen Sie sich beim Betreiber registrieren. Öffnen Sie die Seite http://www.signaturportal.de in einem Webbrowser und wählen Sie die anschließend die Funktionen Kunde werden und Anmelden aus. Einfacher geht es, wenn Sie auf dem Registerblatt Zeitstempeldienst der Konfiguration des OfficeSigners den Link direkt zur Anmeldung verwenden (Abbildung 9). Der OfficeSigner stellt dann eine Verbindung zum Internet her und ruft die Anmeldeseite des Signaturportals (Abbildung 5-40 Registrierung am Signaturportal) auf.

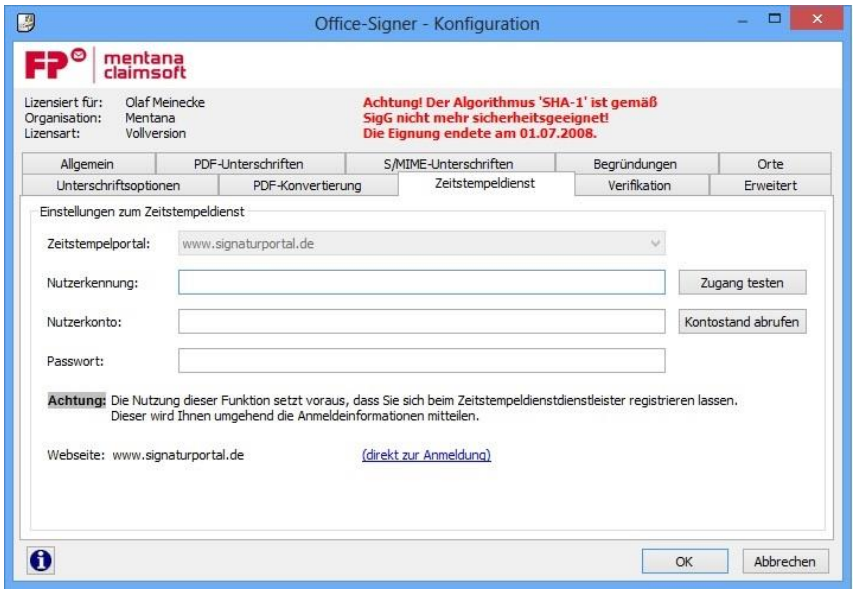

Abbildung 5-39 Konfiguration des Zeitstempeldienstes

Klicken Sie auf der Registrierungsseite des Signaturportals auf weiter, um der der Registrierung zu beginnen. Auf der folgenden Seite werden Sie aufgefordert Ihre Daten zu erfassen. Geben Sie Ihren gewünschten Benutzernamen, Ihre Anschrift sowie Ihre Email-Adresse ein. Klicken Sie auf weiter um die Registrierung abzuschließen. Ihre Eingaben werden gesichert übertragen. Das System wird Sie anschließend per Email über die folgenden Schritte informieren. Notieren Sie sich nach Abschluss der Anmeldung die folgenden Angaben:

- Ihren persönlichen Benutzernamen
- Ihre Kundennummer
- Ihr Passwort

Abbildung 5-40 Registrierung am Signaturportal

Bevor Sie erstmalig einen Zeitstempel für ein Dokument erzeugen können, müssen Sie Ihre Anmeldedaten im OfficeSigner hinterlegen. Öffnen Sie das Kontext-Menü einer beliebigen Datei und wählen Sie aus dem Menü des OfficeSigner die Funktion Einstellungen. Klicken Sie anschließend auf die Registerkarte Zeitstempeldienst und geben Sie Ihre Anmeldedaten in die entsprechenden Felder ein (Abbildung 100). Klicken Sie nach der Eingabe auf die Schaltfläche Zugang testen um die Korrektheit Ihrer Angaben zu überprüfen (Abbildung 1027). Nach erfolgreichem Abschluss dieses Konfigurationsschrittes können Sie den Zeitstempeldienst verwenden. Anschließend können Sie ihr aktuelles Guthaben überprüfen. Klicken Sie die Schaltfläche Kontostand abrufen an. Der OfficeSigner baut eine Netzwerkverbindung zum Zeitstempeldienst auf und fragt Ihre aktuellen Kontodaten ab. Diese werden Ihnen angezeigt (Abbildung 101). Sollte Ihr Zeitstempelguthaben erschöpft sein, so können Sie Ihr Konto jederzeit unter www.signaturportal.de wieder aufladen.

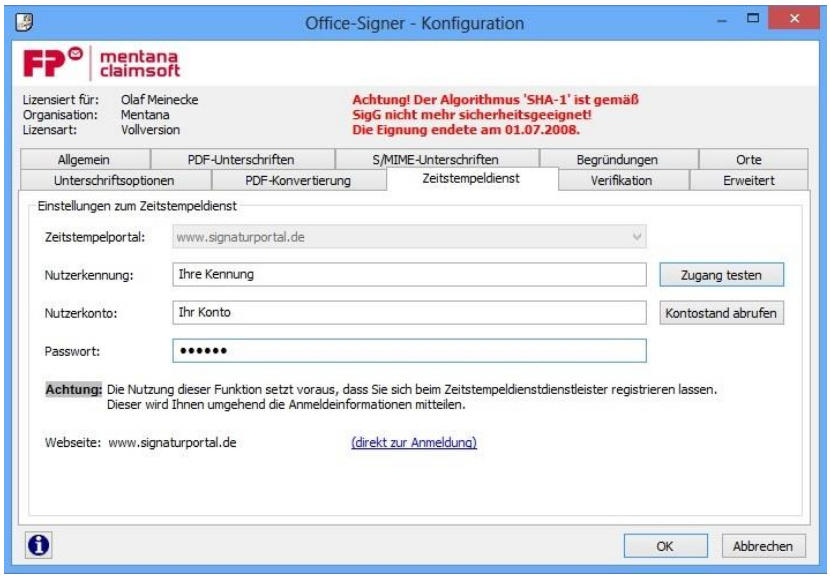

Abbildung 5-41 Zeitstempeldienst mit erfassten Daten

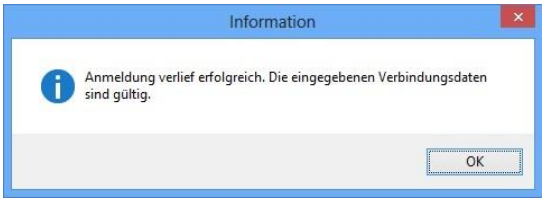

Abbildung 5-42 Verbindungstest zum Zeitstempeldienst

Abbildung 5-43 Kontostand beim Signaturportal

5.9 KONFIGURATION VERIFIKATION

Wählen Sie die Registerkarte Verifikation um Einstellungen für die Überprüfung von elektronischen Signaturen vorzunehmen (Abbildung 103). Sie können auf dieser Seite die folgenden Vorgaben konfigurieren:

- Verifikationsmethode
- Zertifikatsprüfung

- Angaben zu den Stylesheets für die Protokolle

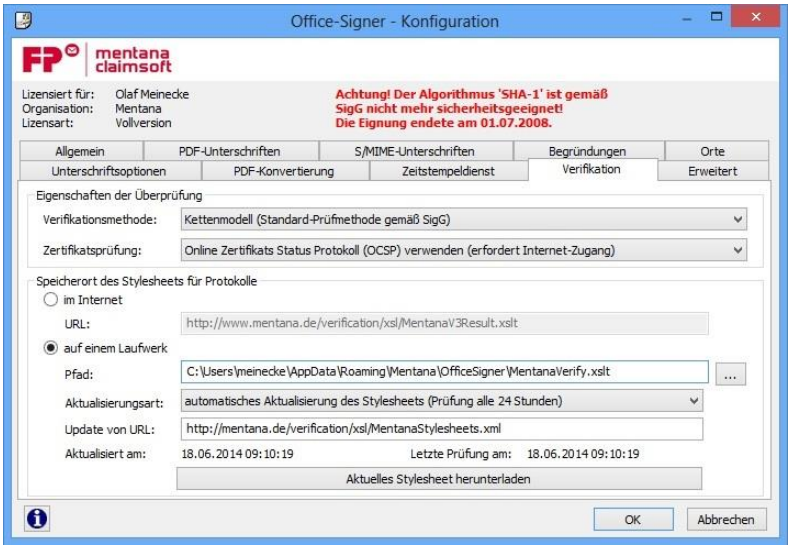

Abbildung 5-44 Konfiguration der Verifikation

5.9.1 EIGENSCHAFTEN DER ÜBERPRÜFUNG

Verifikationsmethode

Wählen Sie aus dieser Liste die zu verwendende Prüfpolitik aus (Abbildung 103):

- **Kettenmodell:** Es wird entlang der Zertifikatskette geprüft, ob das Unterzeichnerzertifikat zum Zeitpunkt der Unterzeichnung und die übergeordneten Zertifikate zum Zeitpunkt der Zertifikatsausstellung gültig waren. Die Verifikation nach dieser Prüfmethode wird vom Signaturgesetz gefordert.
- **erweitertes Schalenmodell:** Es wird überprüft, ob keines der Zertifikate zum Zeitpunkt der Unterzeichnung abgelaufen oder durch Nennung auf einer Sperrliste gesperrt war. Diese Prüfmethode ist strikter als das Kettenmodell.

Zertifikatsprüfung

Zertifikatssperrlisten automatisch überprüfen: Wenn Sie diese Option zulassen, wird der OfficeSigner die im Zertifikat hinterlegten Sperrlistenverteilungspunkte aufsuchen und aktuelle Sperrlisten herunterladen. Die Prüfung der Unterschrift findet anschließend unter Berücksichtigung dieser Sperrlisten (CRL) statt. Das Signaturgesetz fordert die Überprüfung der Sperrlisten.

5.9.2 SPEICHERORT STYLESHEETS PROTOKOLLE

Allgemein kann man hier zuerst festlegen, ob das Stylesheet für die Anzeige eines Verifikationsprotokolls aus dem Internet, oder vom lokalen Laufwerk geladen wird.

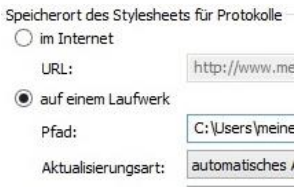

Abbildung 5-45 Speicherort Stylesheet

Die Default-Vorgabe für die Internet-URL lautet: `http://www.mentana.de/verification/xsl/VerificationResult14.xslt`.
Es können hier aber auch andere Stylesheets verwendet werden.

Entscheidet man sich für die Benutzung eines Stylesheets vom lokalen Laufwerk, so kann man direkt angeben, bzw. über einen Datei-Aussuchen-Dialog auswählen wo das Stylesheet auf dem lokalen Laufwerk gespeichert werden soll.

Weiterhin kann man auswählen, wie oft die lokale Version des Stylesheets aktualisiert werden soll.

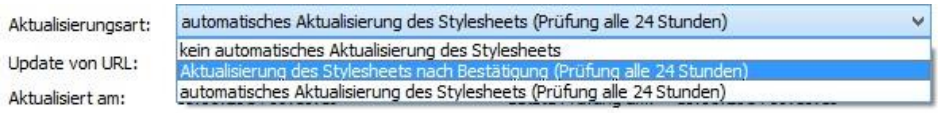

Abbildung 5-46 Aktualisierung des Stylesheets

Hierfür wird auch eine URL benötigt, wo die lokale Version mit der Online-Version verglichen wird (in Abhängigkeit von der Sprache).

Darunter wird angezeigt, wann die letzte Prüfung und die letzte Aktualisierung des Stylesheets erfolgte.

Über die Schaltfläche Aktuelles Stylesheet herunterladen kann man die lokale Version aktualisieren. Anderfalls erfolgt die Aktualisierung entsprechend den Einstellungen bei der Verifikation.

5.10 ERWEITERTE KONFIGURATION

Auf der Seite „Erweitert“ der Konfiguration kann man die Sprache des OfficeSigners einstellen

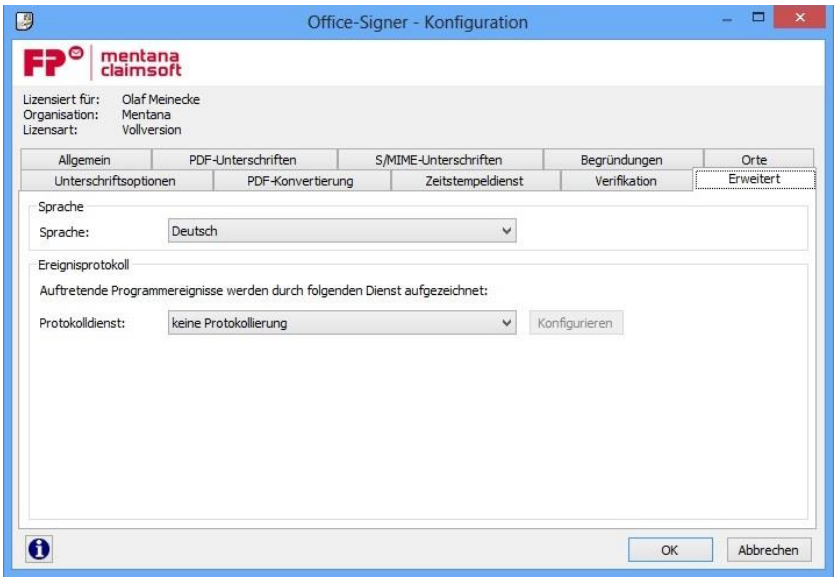

Abbildung 5-47 Konfiguration Seite „Erweitert“

Zusätzlich kann man das Protokollieren in einem Ereignisprotokoll mitloggen. Hierbei gibt es zwei Möglichkeiten:

- Textdatei
- Datenbank

Textdatei als Log-Datei:

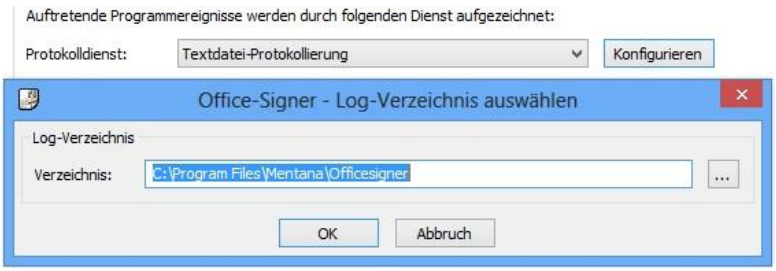

Abbildung 5-48 Textdatei-Protokollierung Einstellungen

Logging in eine Datenbank:

Abbildung 5-49 Datenbank für Logging

Für die Verbindung wird eine ODBC-Datenquelle benötigt. Nähere Angaben hierzu erhalten Sie über unseren Support.

6 STICHWORTVERZEICHNIS

Befehlszeile 63
eingebetteten S/MIME Signatur 37
eingebetteten sichtbaren Signatur 32
erweitertes Schalenmodell 94
Externe Signatur 25
Hashwert 57
Integrität 42
Interne Signatur 25
Kettenmodell 94
Lizenzbedingungen 13
Namensgleichheit 43
Office-Cryptor 14
Parameter 63
Sperrlistenvermerke 43
Stapelsignatur 40
Unterschriftsposition 76
Verifikation 44
Verifikationsmechanismen 42
Verifizieren 43
XML -Datei 51, 54
Zeitstempel 55
Zertifikatsgültigkeit 43
Zertifikatskette 43

7 ABBILDUNGSVERZEICHNIS

Abbildung 3-1 Setup-Icon 12
Abbildung 3-2 Willkommen-Fenster 12
Abbildung 3-3 Installationsfenster mit Lizenzvereinbarung 13
Abbildung 3-4 Installationsfenster mit Komponentenauswahl 14
Abbildung 3-5 Installationsfenster mit benutzerdefinierter Installation 15
Abbildung 3-6 Vorbereitung Installation abgeschlossen 15
Abbildung 3-7 Abfrage Benutzerkontensteuerung Windows 7 16
Abbildung 3-8 Installationsverlauf 16
Abbildung 3-9 Installationsende 17
Abbildung 3-10 Noch keine, bzw. ungültige Lizenz 18
Abbildung 3-11 Lizenz-Datei öffnen 18
Abbildung 3-12 gültige Lizenz 19
Abbildung 3-13 Softwarezertifikat installieren (Kontextmenü) 19
Abbildung 3-14 Zertifikatsimport - Willkommen 20
Abbildung 3-15 Zertifikatimport-Assistent 20
Abbildung 3-16 Zertifikatsimport – Kennworteingabe 21
Abbildung 3-17 Zertifikatsimport - Zertifikatsspeicher 22
Abbildung 3-18 Zusammenfassung Zertifikatimport-Assistent 22
Abbildung 3-19 Zertifikatsimport – Sicherheitswarnung 23
Abbildung 3-20 Meldung einer erfolgreichen Zertifikats-Installation 23
Abbildung 3-21 Details der digitalen Signatur 25
Abbildung 4-1 Infos über Zertifikat 26
Abbildung 4-2 Zertifikat auswählen 27
Abbildung 4-3 Unterschriftstyp 27
Abbildung 4-4 Unterschriftstyp auswählen 28
Abbildung 4-5 Unterschriftsfelder 29
Abbildung 4-6 Begründung auswählen 29
Abbildung 4-7 Ort auswählen 30
Abbildung 4-8 Zusammenfassung für die Unterschrift 31
Abbildung 4-9 Signaturwarndialog 31
Abbildung 4-10 Bestätigung bei erfolgreicher Unterschrift 32
Abbildung 4-11 Unterschrift im PDF-Dokument (Ansicht Adobe PDF-Reader) 32
Abbildung 4-12 Zertifikat auswählen für Signatur 33
Abbildung 4-13 Unterschriftstyp und Unterschriftsposition selektieren 33
Abbildung 4-14 Begründung und Ort der Signatur 34
Abbildung 4-15 Zusammenfassung zur eingebetteten, sichtbaren Signatur 34
Abbildung 4-16 Signaturwarndialog vor Signatur 35
Abbildung 4-17 Bestätigung nach erfolgter Signatur 35
Abbildung 4-18 sichtbare Unterschrift im PDF-Dokument (Ansicht Adobe PDF-Reader) 36
Abbildung 4-19 sichtbare Unterschrift mit Hintergrundbild in PDF-Dokument 37
Abbildung 4-20 Zertifikat auswählen 38

Abbildung 4-21 Unterschriftstyp wählen 38
Abbildung 4-22 Zusammenfassung 39
Abbildung 4-23 Signaturwarndialog 39
Abbildung 4-24 Bestätigung nach erfolgter Signatur 39
Abbildung 4-25 Dateiliste mit externer Signatur 40
Abbildung 4-26 Dateiliste bei Stapelsignatur 40
Abbildung 4-27 Einstellungen PDF-Dokumente 41
Abbildung 4-28 Einstellungen nicht PDF-Dokumente 41
Abbildung 4-29 Signaturwarndialog 42
Abbildung 4-30 Signaturergebnisse 42
Abbildung 4-31 OfficeSigner - Menü – Verifizieren (Kontextmenü) 43
Abbildung 4-32 Fortschrittsanzeige Verifikation 44
Abbildung 4-33 Verifikationsergebnis 44
Abbildung 4-34 Testergebnis 45
Abbildung 4-35 Protokoll speichern 45
Abbildung 4-36 Dateiliste mit Verifikationsprotokoll 46
Abbildung 4-37 Verifikations-Protokoll mit fehlendem xslt-Style-Sheet 46
Abbildung 4-38 Manueller Eingriff in das Verifikations-Protokoll 47
Abbildung 4-39 XML-Anzeige im Internet-Explorer ohne xslt-Verweis 47
Abbildung 4-40 Anzeige Verzeichnis mit PDF, Verifikationsprotokoll und xslt-Datei 48
Abbildung 4-41 Verifikationsprotokoll 48
Abbildung 4-42 OfficeSigner-Menü – Verifizieren (Kontextmenü) 50
Abbildung 4-43 Verifikationsergebnis 50
Abbildung 4-44 Dateidialog Protokoll speichern 51
Abbildung 4-45 Dateiliste mit externer Signatur und Protokolldatei 51
Abbildung 4-46 Verifikationsprotokoll 52
Abbildung 4-47 OfficeSigner-Menü – De-Mail verifizieren (Kontextmenü) 52
Abbildung 4-48 Verifikationsergebnis De-Mail 53
Abbildung 4-49 Dateidialog Protokoll speichern (De-Mail) 53
Abbildung 4-50 Dateiliste mit De-Mail und Protokolldatei 54
Abbildung 4-51 De-Mail Verifikationsprotokoll 54
Abbildung 4-52 Startseite Signaturportal 55
Abbildung 4-53 OfficeSigner-Menü – Zeitstempel (Kontextmenü) 56
Abbildung 4-54 Verlaufsanzeige Zeitstempelanforderung 56
Abbildung 4-55 Zeitstempel erfolgreich angefordert 56
Abbildung 4-56 Dateiliste mit Zeitstempeldatei 57
Abbildung 4-57 Hashwert berechnen 57
Abbildung 4-58 Hashwert Berechnungsverfahren auswählen 58
Abbildung 4-59 OfficeSigner-Menü - Info 59
Abbildung 4-60 Info mit Lizenz 59
Abbildung 4-61 Lizenzmanager ohne Lizenz 60
Abbildung 4-62 Lizenz-Datei öffnen 60

Abbildung 4-63 Lizenzmanager mit gültiger Lizenz 61
Abbildung 4-64 Info mit gültiger Lizenz 61
Abbildung 4-65 Anhang einfügen 62
Abbildung 4-66 Anhang auswählen 62
Abbildung 4-67 Bestätigung bei erfolgreich eingefügter Datei 63
Abbildung 4-68 PDF-Dokument mit Anhang (Adobe Reader) 63
Abbildung 4-69 geöffneter Anhang des PDF-Dokumentes 63
Abbildung 5-1 OfficeSigner Konfiguration 66
Abbildung 5-2 Infobildschirm OfficeSigner 66
Abbildung 5-3 Seite „Allgemein" der Konfiguration 67
Abbildung 5-4 Konfiguration OfficeSigner allgemein Bereich Benutzerzertifikate 68
Abbildung 5-5 Geöffnete Zertifikatsliste zur Auswahl 68
Abbildung 5-6 Weitere Informationen zu einem Zertifikat 69
Abbildung 5-7 Auswahl Hash-Algorithmus für Signatur 69
Abbildung 5-8 Meldung bei Wahl vom SHA-1-Algorithmus (veraltet) 70
Abbildung 5-9 Auswahl Anzeige CSP in Zertifikatsliste 70
Abbildung 5-10 Bedingung der Dokumentenprüfung vor einer Signatur 70
Abbildung 5-11 Prüfungsmethode für Dokumente vor einer Signatur 71
Abbildung 5-12 Konfiguration Allgemein-Ausgaben nach der Signatur 71
Abbildung 5-13 Konfiguration der PDF-Unterschriften 72
Abbildung 5-14 Konfiguration der S/Mime-Signatur 73
Abbildung 5-15 Konfiguration der Begründungen 73
Abbildung 5-16 Begründung erfassen 74
Abbildung 5-17 Bearbeiten einer Begründung 74
Abbildung 5-18 Als Standard ausgewählte Begründung 75
Abbildung 5-19 Konfiguration der Orte 75
Abbildung 5-20 Konfiguration der Unterschriftspositionen 77
Abbildung 5-21 Hinzufügen einer Unterschriftsposition 77
Abbildung 5-22 Werte der Unterschriftsposition bei Positionierung unten links 79
Abbildung 5-23 Werte der Unterschriftsposition bei Positionierung unten rechts 79
Abbildung 5-24 Werte der Unterschriftsposition bei Positionierung oben links 80
Abbildung 5-25 Werte der Unterschriftsposition bei Positionierung oben rechts 80
Abbildung 5-26 Bearbeiten einer Unterschriftsposition 81
Abbildung 5-27 Hintergrundbild öffnen 81
Abbildung 5-28 Liste der Unterschriftspositionen 82
Abbildung 5-29 Unterschriftsoptionen 83
Abbildung 5-30 Logo-Konfiguration 84
Abbildung 5-31 Hintergrund-Grafik 84
Abbildung 5-32 Feldliste 85
Abbildung 5-33 Eigenschaften eines Signaturfeldes 85
Abbildung 5-34 Liste der Feldwerte 86
Abbildung 5-35 Feldliste mit einem Eintrag 87

Abbildung 5-36 Beispiel einer XML-Datei....88
Abbildung 5-37 Bemaßung Signatur- und Textfelder....89
Abbildung 5-38 PDF-Konvertierung....90
Abbildung 5-39 Konfiguration des Zeitstempeldienstes....91
Abbildung 5-40 Registrierung am Signaturportal....92
Abbildung 5-41 Zeitstempeldienst mit erfassten Daten....93
Abbildung 5-42 Verbindungstest zum Zeitstempeldienst....93
Abbildung 5-43 Kontostand beim Signaturportal....93
Abbildung 5-44 Konfiguration der Verifikation....94
Abbildung 5-45 Speicherort Stylesheet....95
Abbildung 5-46 Aktualisierung des Stylesheets....95
Abbildung 5-47 Konfiguration Seite „Erweitert“....96
Abbildung 5-48 Textdatei-Protokollierung Einstellungen....96
Abbildung 5-49 Datenbank für Logging....97

Stand: 27.03.2017 16:21