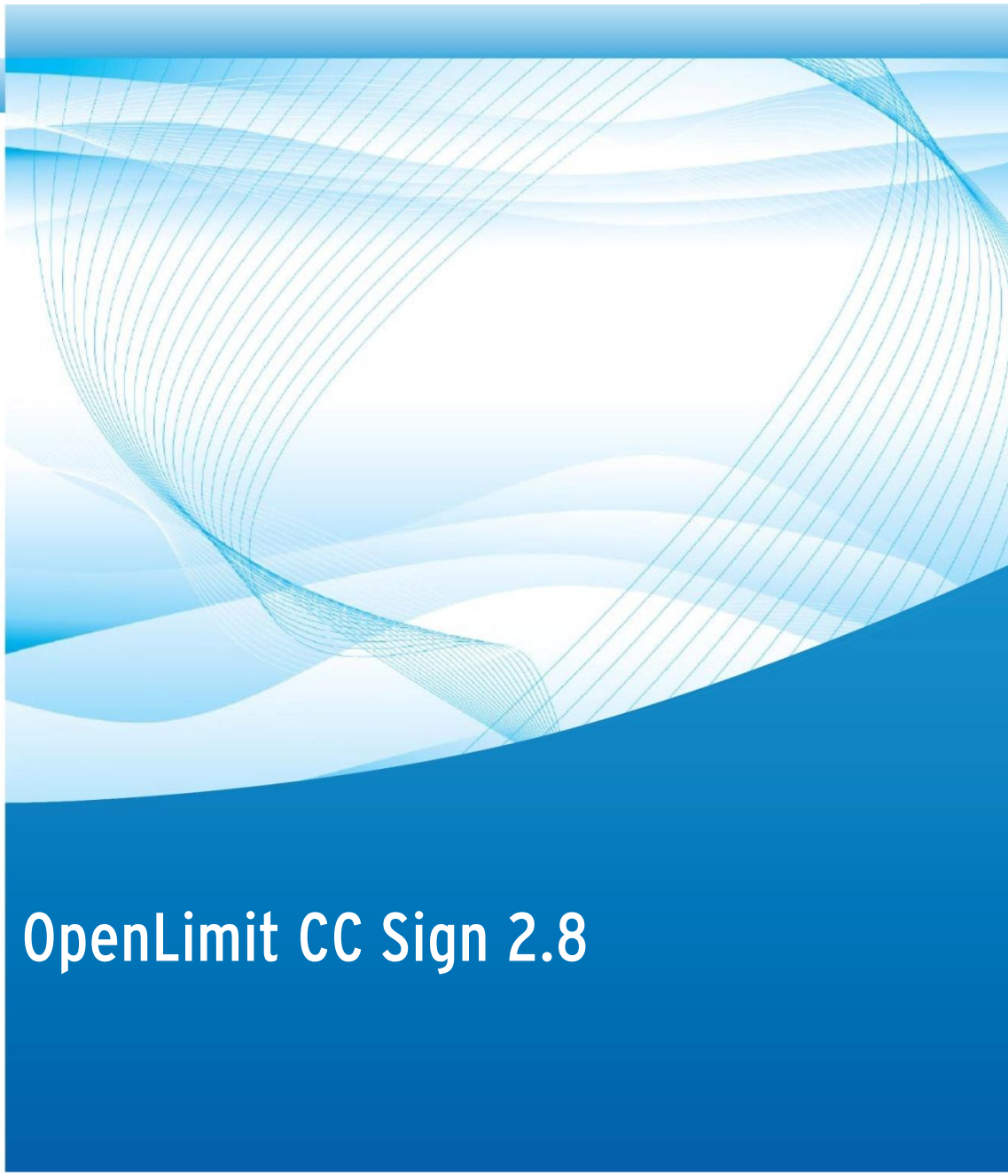
Elektronisches Handbuch



OpenLimit CC Sign 2.8

Version 1.0 Stand: 01.10.2014

Diese Dokumentation bietet dem Anwender eine Anleitung zur Arbeit mit dem Produkt OpenLimit CC Sign Version 2.8. In Einzelfällen kann es zu Abweichungen zwischen den beschriebenen Abläufen, der Dokumentation und der tatsächlichen Anwendung kommen. Die OpenLimit SignCubes AG übernimmt keine Haftung für etwaige Abweichungen und deren Folgen. Da die Software ständig weiter entwickelt wird, behält sich die OpenLimit SignCubes AG Änderungen am Inhalt der Dokumentation ohne Ankündigung vor.

Die OpenLimit SignCubes Basiskomponenten 2.8, Version 2.8.0.1 basieren auf den OpenLimit SignCubes Basiskomponenten 2.5, Version 2.5.0.4, die einer Evaluierung nach Common Criteria v2.3 mit Prüfniveau EAL4+ unterzogen wurden und eine Sicherheitsbestätigung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) erhalten haben. Für die OpenLimit SignCubes Basiskomponenten 2.8, Version 2.8.0.1 wurde durch die OpenLimit SignCubes GmbH eine Herstellerklärung abgegeben. Mehr Informationen zur Produktzertifizierung bzw. Herstellerklärung finden Sie auf den Webseiten des Bundesamtes für Sicherheit in der Informationstechnik (BSI) unter http://www.bsi.de und der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Bundesnetzagentur) unter http://www.bundesnetzagentur.de.

Hinweise und Kommentare richten Sie bitte an **documentation@openlimit.com**.

OpenLimit SignCubes AG
Zugerstraße 76 B
CH - 6341 Baar
Schweiz

www.openlimit.com

Inhaltsverzeichnis

Glossar

CC	Die Common Criteria ist ein internationales Normen- und Regelwerk, welches Vorgaben zur sicherheitstechnischen Untersuchung von IT Produkten definiert.
CRL	Eine Certificate List ist eine Liste, die von einem Zertifikatsanbieter herausgegeben wird und eine Liste aller Zertifikate enthält, die zum Zeitpunkt des Abrufs der Sperrliste durch den Inhaber des Zertifikats gesperrt worden ist.
OCSP	Online Certificate Status Protocol ist ein Protokoll, welches über eine Online Abfrage die Möglichkeit bietet, bei dem Herausgeber zu erfragen, ob ein Zertifikat bekannt bzw. gesperrt ist. Dieses verfahren wird als sogenannte Positiv-Auskunft bezeichnet.
RSA	Kryptographische Mechanismen, benannt nach den Erfindern Ronald L. **R**ivest, Adi **S**hamir und Leonard **A**dleman
ECDSA	Elliptic Curve Digital Signature Algorithm, kryptographische Mechanismen basierend auf elliptischen Kurven
CMS	Cryptographic Message Syntax – beschreibt das Standardformat für kryptographische Nachrichten

1 Einleitung

Die OpenLimit SignCubes Basiskomponenten 2.8, Version 2.8.0.1 sind Bestandteil des Produktes OpenLimit CC Sign 2.8, das Sie auf CD-ROM oder Online von der OpenLimit SignCubes AG oder einem ihrer Reseller erworben haben. Zu dem Produkt werden als Dokumentation die „Online Help“ und der „OpenLimit User Guide“ mitgeliefert. In der „Online Help“ sind alle sicherheitsrelevanten Funktionen beschrieben, auf die sich die Herstellererklärung beziehen Das betrifft insbesondere die folgenden Komponenten:

- den OpenLimit SignCubes Security Environment Manager
- den OpenLimit SignCubes Viewer
- das OpenLimit SignCubes Integrity Tool

Darüber hinaus gibt die „Online Help“ Hinweise zur korrekten und sicheren Konfiguration des Produktes. Weiterhin werden in der „Online Help“ alle Fehlermeldungen aufgelistet und Hinweise zum korrekten Umgang mit Fehlermeldungen gegeben.

Bevor Sie anfangen, mit dem Produkt zu arbeiten, lesen Sie bitte die folgenden Kapitel in der „Online Help“ aufmerksam durch:

- Bevor Sie beginnen
- Mindestanforderungen und Sicherheitsmaßnahmen
- Sicherheitskomponenten der OpenLimit SignCubes Basiskomponenten 2.8, Version 2.8.0.1
- Konfiguration der OpenLimit SignCubes Basiskomponenten

Eine Anleitung zum Umgang mit dem Produkt sowie der Nutzung einzelner Funktionen im Detail, finden Sie in der „Online Help“ im Kapitel „Arbeiten mit den OpenLimit SignCubes Basiskomponenten 2.8, Version 2.8.0.1“.

Die folgenden Abschnitte beschreiben den Umgang mit den einzelnen Bestandteilen des Produktes OpenLimit CC Sign 2.8. Dieses Kapitel soll Ihnen den Umgang mit dem Produkt erleichtern und Ihnen dabei helfen, schnell mit den einzelnen Programmfunktionen vertraut zu werden.

Die Arbeitsabläufe unter den verschiedenen Modulen der OpenLimit SignCubes Software sind immer wieder dieselben. Deshalb beschreiben wir in diesem separaten Kapitel nur die immer wiederkehrenden Abläufe.

2 Dateiformate

Die OpenLimit SignCubes Software 2.8 speichert Daten in verschiedenen Dateiformaten ab. Das Format können Sie über den OpenLimit SignCubes Security Environment Manager einstellen. Standardmäßig wird bei der Installation der Software das Format so eingestellt, dass die Signaturdatei und die Originaldaten in einer Datei gespeichert werden.

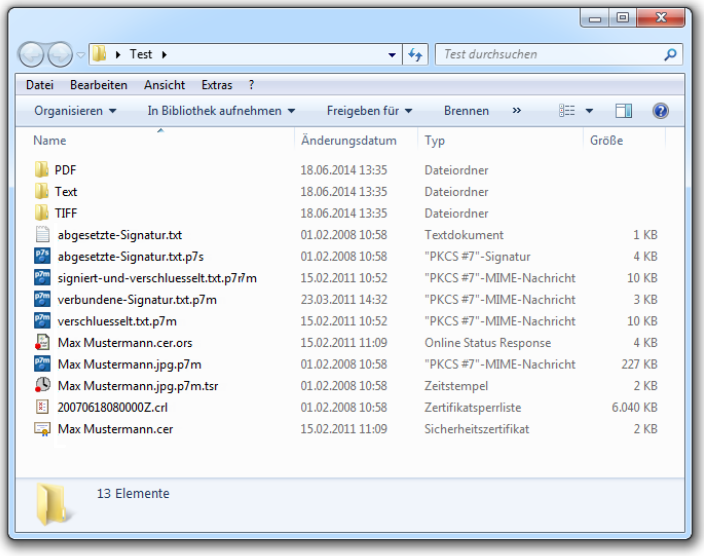
p7s - Format

*.p7s-Dateien sind PKCS#7-Daten: Es handelt sich dabei um eine abgesetzte Signatur (detached signature). Das heißt, die signierten Daten und die Signatur sind in zwei getrennten Dateien gespeichert. Diese Vorgehensweise hat den Vorteil, dass man sich die Originaldaten mit dem dazugehörigen Programm ansehen kann. Solange diese nicht geändert werden, bleibt auch die Signatur gültig. Die Signatur ist mit der Originaldatei durch denselben Dateinamen verbunden. Wenn Sie eine p7s Datei mit einem Doppelklick öffnen, wird automatisch die Signaturprüfung gestartet.

p7m - Format

*.p7m-Dateien sind PKCS#7-Daten: Dahinter können sich signierte, verschlüsselte oder signierte und verschlüsselte Daten verbergen.

Signierte bzw. signierte und verschlüsselte p7m-Dateien liegen als Verbund-Dateien vor. Das heißt, die Datei beinhaltet sowohl eine oder mehrere Signaturen im p7s-Format als auch die Originaldaten, welche signiert oder signiert und verschlüsselt wurden. Wenn Sie eine p7m-Datei doppelklicken, wird die Datei entschlüsselt, sofern sie verschlüsselt war.



Hinweis: Verschlüsselte Daten werden immer als *.p7m Datei gespeichert. Für die Signaturerzeugung mit der OpenLimit SignCubes Shellextension können Sie zwischen p7s (Daten und Signatur getrennt) oder p7m (Daten und Signatur verbunden) wählen, indem Sie zuvor die Einstellungen über das OpenLimit Icon ändern.

ors - Format

*.ors Dateien sind Online-Statusabfragen zu Zertifikaten. Der Status eines Zertifikats kann bei der Signaturerstellung oder -prüfung vom Trustcenter abgefragt werden und gibt eine Aussage über die Gültigkeit des Zertifikats.

tsr - Format

*.tsr Dateien sind Zeitstempelinformationen. Zur Erzeugung von Zeitstempeln benötigt der User einen speziell freigeschalteten Zugriff auf einen Zeitstempel-Dienst. Ein Zeitstempel gibt eine Aussage darüber, dass Dateien zu einem bestimmten Zeitpunkt existiert haben. Dies wird durch eine digital signierte Bescheinigung einer Zertifizierungsstelle bestätigt.

crl - Format

*.crl - Dateien sind Sperrlisten: Durch Anklicken mit der rechten Maustaste wird die Sperrliste geöffnet und Sie können sich weitere Details zu einzelnen Zertifikaten anzeigen lassen.

cer - Format

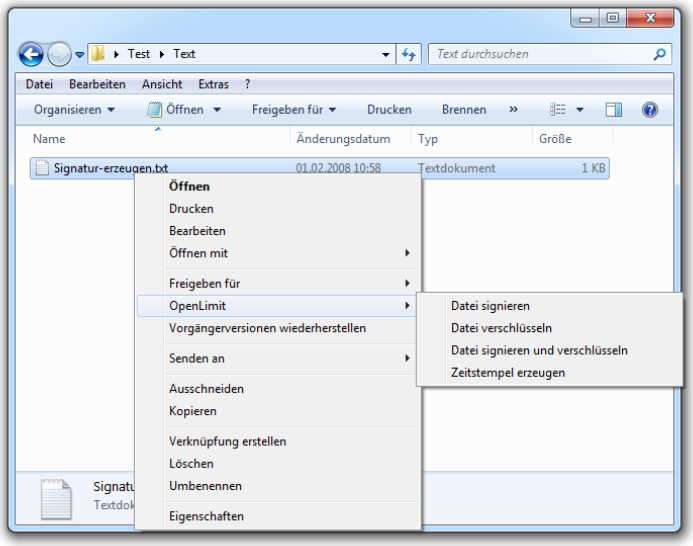
*.cer-Dateien sind Zertifikatsdateien: Mit einem Doppelklick haben Sie die Möglichkeit, sich dieses Zertifikat anzeigen zu lassen.

3 Signatur erzeugen

Die OpenLimit SignCubes Software bietet Ihnen verschiedene Möglichkeiten, qualifizierte Signaturen nach dem deutschem Signaturgesetz zu erstellen. Es können aber auch fortgeschrittene oder andere Signaturen erstellt werden.

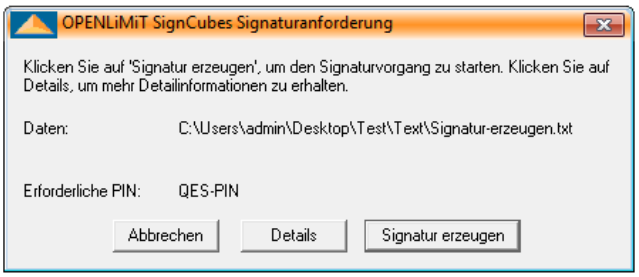
3.1 Signatur erzeugen über die Shellextension

Starten Sie beispielsweise die Signaturerzeugung über die Shellextension, in dem Sie im Dateimanager die zu signierende Datei mit der rechten Maustaste anklicken und **[OpenLimit/Datei signieren]** auswählen.



Unabhängig davon, aus welchem Modul heraus Sie den Vorgang der Signaturerzeugung starten, ist der nachfolgend beschriebene Ablauf immer gleich.

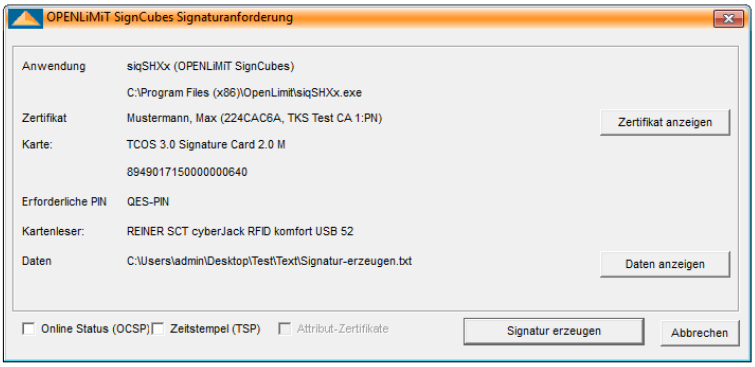
Nach dem Start der Signaturerzeugung öffnet sich das folgende Fenster:



Wenn Sie auf **[Abbrechen]** klicken, wird der Vorgang abgebrochen und keine Signatur erzeugt.

Klicken Sie auf **[Signatur erzeugen]**, wird eine Signatur erzeugt, ohne dass Ihnen weitere Detailinformationen, wie z.B. der verwendete Kartenleser, das Zertifikat und die erforderliche PIN, angezeigt werden. Es erfolgt sofort die Aufforderung zur PIN Eingabe.

Klicken Sie auf den Button **[Details],** so erscheint das nachfolgende Signaturanforderungsfenster, in dem Ihnen weitere Detailinformationen angezeigt werden.



Hier sehen Sie das Zertifikat, welches zur Signaturerzeugung verwendet wird, die Karte, die erforderliche PIN, den Kartenleser und die zu signierenden Daten.

Vor der Signaturerzeugung sollten Sie sich im Fall von Daten im TXT, TIFF oder PDF Format über **[Daten anzeigen]** die zu signierenden Daten im OpenLimit SignCubes Viewer anzeigen lassen, um sicher zu sein, welche Daten Sie tatsächlich signieren. Klicken Sie dazu auf den Button **[Daten anzeigen]**.

Nachdem Sie in diesem Fenster auf **[Signatur erzeugen]** geklickt haben, erscheint die Aufforderung zur PIN Eingabe. Je nach Kartenleser erscheint nun eine unterschiedliche Meldung.

Geben Sie die PIN auf der Tastatur des Kartenlesers ein, eventuell müssen Sie diese mit **[OK]** bestätigen.

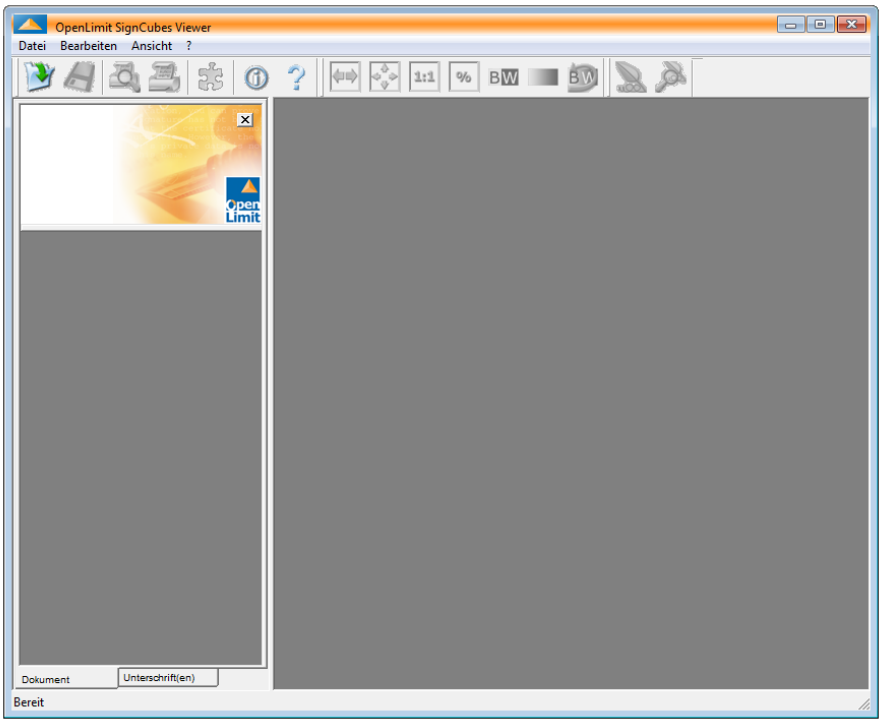
Anschließend erscheint ein Fenster mit der Meldung, dass die Daten signiert wurden.

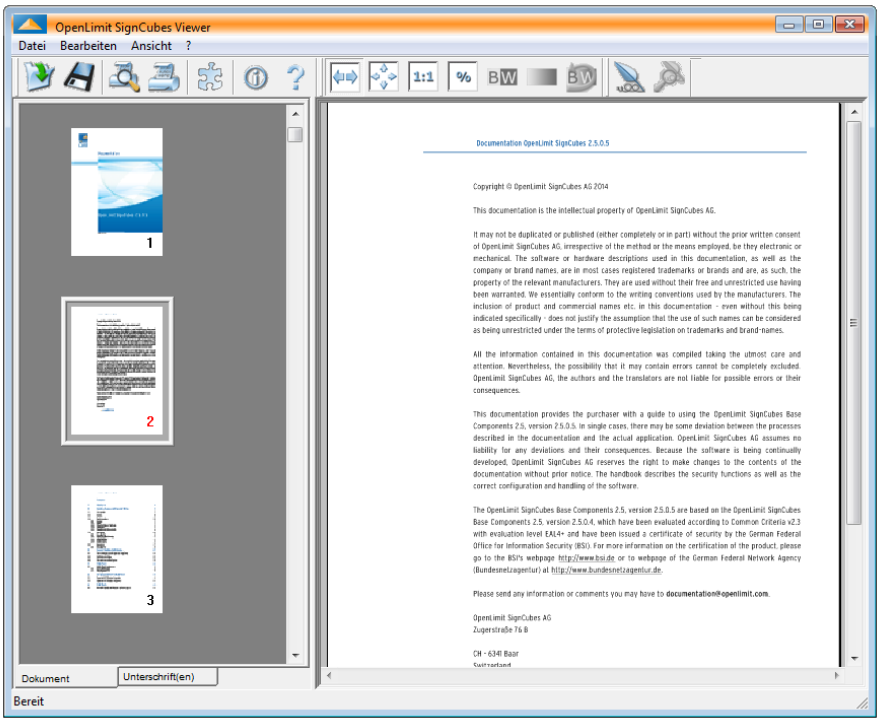
Sollte hier ein Fenster mit der Meldung erscheinen, dass die eingegebene Signatur-PIN zurückgewiesen wurde, dann bedeutet das, dass Sie eine falsche PIN eingegeben haben.

3.2 PDF-Dateien mit dem OpenLimit Viewer signieren

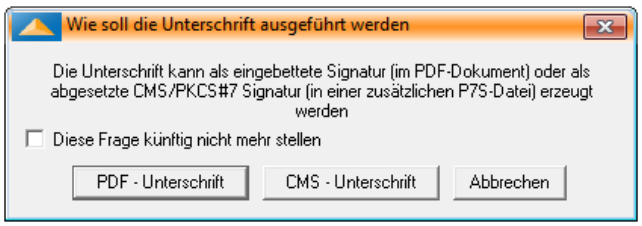
Starten Sie zunächst den OpenLimit Viewer über:

- **[Start/Alle Programme/OpenLimit/OpenLimit Viewer]** bzw. **[Apps/OpenLimit/OpenLimit Viewer]**
- Öffnen Sie eine PDF-Datei über **[Datei/ Öffnen]**.





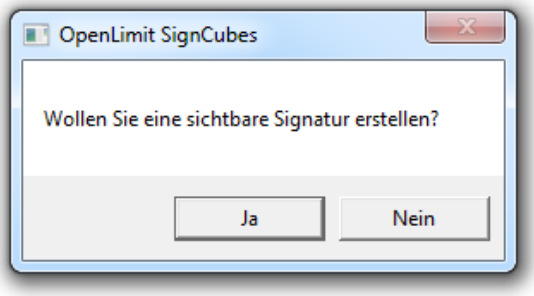
Klicken Sie auf den Button **[Unterschreiben]**. In dem folgenden Auswahldialog wählen Sie **[PDF-Unterschrift]** aus.



Das weitere Vorgehen hängt davon ab, ob das PDF-Formular bereits Unterschriftsfelder enthält oder nicht:

3.2.1 PDF-Formulare ohne Unterschriftsfelder signieren

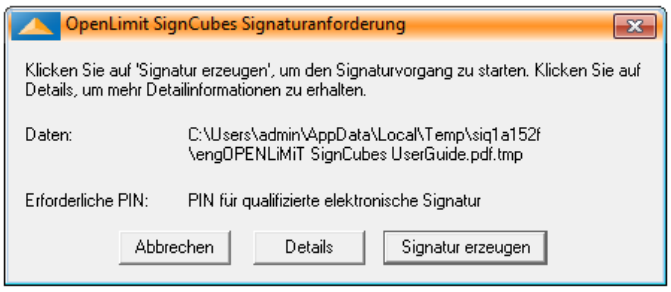
In dem Fall, dass das PDF-Formular keine Unterschriftsfelder enthält bestätigen Sie in dem folgenden Fenster mit **[Ja]** das Erstellen einer sichtbaren PDF-Signatur. Klicken Sie auf **[Nein]**, wenn Sie eine unsichtbare PDF-Signatur erzeugen wollen. Daraufhin folgt sofort der Signaturanforderungsdialog.



Nach Bestätigen mit **[Ja]** werden Sie aufgefordert, die Größe des Signaturfeldes sowie die Position durch Ziehen eines Rechtecks festzulegen.

In dem folgenden Fenster bestätigen Sie die Position mit **[Ja]**. Über **[Nein]** bekommen Sie die Möglichkeit, den Rahmen erneut zu ziehen, über **[Abbrechen]** wird der Vorgang beendet.

Anschließend öffnet sich der Signaturanforderungsdialog.



Über den Button **[Details]** können Sie weitere Einstellungen vornehmen, wie z.B. die Auswahl, ob Sie den Online-Status, Zeitstempel oder das Attributzertifikat in die Signatur einbetten wollen.

Ebenso können Sie sich Informationen, wie die Details zum Zertifikat, welches Sie für die Signaturerzeugung gerade verwenden, die erforderliche PIN, den Kartenleser und die zu signierenden Daten anzeigen lassen.

Klicken Sie auf **[Signatur erzeugen]**. Anschließend werden Sie aufgefordert, die PIN einzugeben. Je nach Kartenleser erscheinen hierfür unterschiedliche Meldungen.

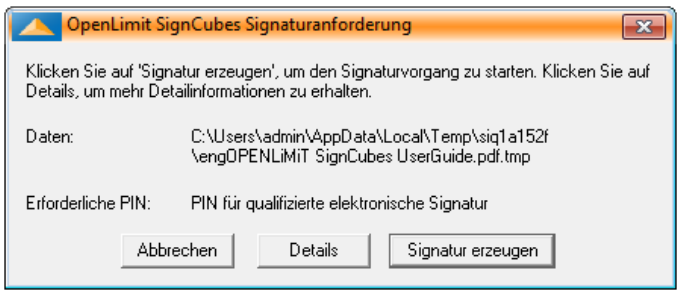
Geben Sie die PIN über die Tastatur des Kartenlesers ein. Eventuell müssen Sie diese durch eine OK-Taste (oder grüner Haken) bestätigen.

Daraufhin wird die Signatur erzeugt und es erscheint ein Fenster mit der Meldung, dass die Daten signiert wurden.

Klicken Sie **[OK]** und beenden Sie den OpenLimit Viewer. Die signierte PDF-Datei wird automatisch gespeichert.

3.2.2 PDF-Formulare mit Unterschriftsfeldern signieren

Sind in dem PDF-Formular bereits Unterschriftsfelder generiert und Sie haben zum 1. Mal PDF Unterschrift ausgewählt, dann wird sofort der Signaturanforderungsdialog angezeigt.



Nach Bestätigen des Button Signatur erzeugen und der erfolgreichen PIN Eingabe wird die Signatur in dem 1. vorhandenen Unterschriftsfeld eingefügt. Bei der 2. Signatur wird automatisch das 2. Unterschriftsfeld ausgewählt usw.

3.2.3 PDF Unterschriftsfelder über Platzhalter definieren

Über die Konfigurationsdatei „sigSignature.cfg“, die mit der Installation der Software von OpenLimit CC Sign 2.8 in dem Programmeordner abgelegt wird, haben Sie die Möglichkeit, ein bzw. mehrere Unterschriftsfelder für eine PDF-Datei über Platzhalter zu definieren. In der „sigSignature.cfg“ finden Sie einen Abschnitt:

```
[Auto]
search=true
Text=.....................................................
Width=200
Height=50
```

In diesem Beispiel wird bei der Signaturerzeugung in der PDF-Datei über der Zeile mit den 56 Punkten automatisch ein Unterschriftsfeld generiert und die Signatur in diesem Feld platziert. Bei einer zweiten Signatur wird wiederum nach der Zeichenkette gesucht. Falls diese nicht vorhanden ist, haben Sie die Möglichkeit, mit der Maustaste einen Rahmen für das Unterschriftsfeld zu ziehen.

Diese Funktionalität können Sie z.B. nutzen, indem Sie zunächst Ihr Dokument in Word erstellen und für die Unterschriftsfelder eine entsprechende Zeichenfolge setzen, die identisch ist mit dem Wert für den Parameter „Text“ in der „sigSignature.cfg“. Anschließend drucken Sie die Worddatei über den OpenLimit PDF Producer. Damit öffnet sich der OpenLimit Viewer und zeigt Ihnen die PDF-Datei an. Klicken Sie jetzt auf Unterschreiben und wählen PDF-Signatur, so wird das Unterschriftsfeld automatisch an der Stelle mit der Zeichenkette erstellt und die Signatur platziert.

Falls Sie die weiteren Möglichkeiten der Konfiguration von Unterschriftsfeldern nutzen wollen, fordern Sie bitte die detaillierte Dokumentation an, über:

- info@openlimit.com

3.3 Signaturen prüfen

Die Prüfung einer Signatur erfordert Sorgfalt und Umsicht. Folgende Punkte sollten geprüft werden:

- Ist das Dokument wirklich unverändert?
- Ist der Signaturinhaber echt?
- Ist das Zertifikat gesperrt?

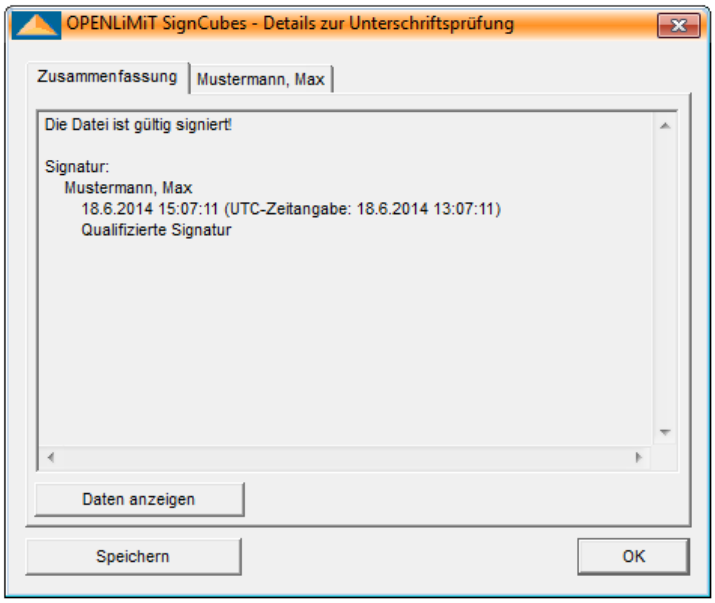
Einige Teile der Prüfung werden automatisch von der Software vorgenommen. Qualifizierte Signaturen nach dem deutschen Signaturgesetz lassen sich lückenlos zurückverfolgen bis zur Bundesnetzagentur. Das Herausgeberzertifikat der Bundesnetzagentur ist in die Software integriert. Dieser Zertifizierungspfad muss mathematisch korrekt und lückenlos sein. Aber auch andere Wurzelzertifikate können im Betriebssystem als vertrauenswürdig definiert werden.

Deshalb bleibt es grundsätzlich dem Benutzer überlassen, welchen Zertifikaten er vertraut und welchen nicht.

Weitere Informationen zu den Abläufen der Signaturprüfung und der Public Key Infrastruktur finden Sie unter „Grundlagen der elektronischen Signatur“ in der „Online Help“.

3.3.1 Zusammenfassung

Nachdem Sie auf **[Signatur Prüfen]** geklickt haben, erscheint der Dialog **Details zur Signaturprüfung**:



In der Zusammenfassung der Signaturprüfung steht zunächst, ob die Signatur **gültig**, **ungültig** oder **mathematisch korrekt** ist.

Wenn bei der Prüfung einer qualifizierten Signatur kein Signaturerstellungszeitpunkt vorliegt (also in der Signatur enthalten ist), kann nicht sichergestellt werden, ob die qualifizierte Signatur zum Zeitpunkt ihrer Erstellung auf einem gültigen qualifizierten Zertifikat beruhte. Bitte wenden Sie sich an die Bundesnetzagentur, um weiterführende Informationen zur Interpretation dieses technischen Umstands zu erhalten.

Wenn die Anzeige der Signaturprüfung eine Signatur als **ungültig** ausweist, können Sie die zutreffende Ursache ermitteln, indem Sie das Register mit dem Namen des Signaturzertifikatinhabers auswählen. Dort werden Ihnen die zugehörigen Detailinformationen angezeigt. Einer oder beide der folgenden Fälle sind eingetreten:

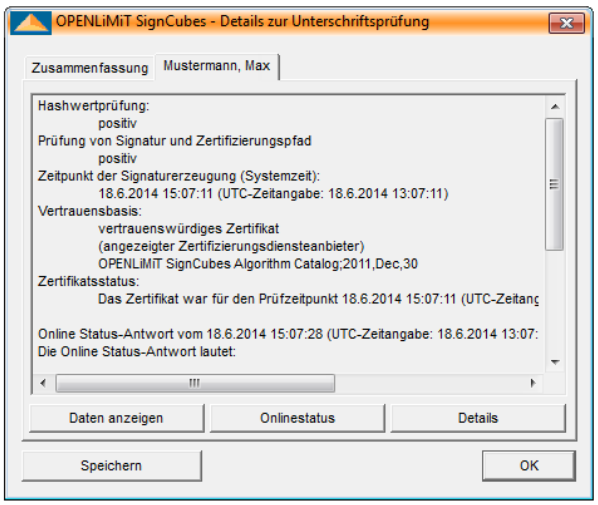
- Das Ergebnis der Hashwertprüfung ist negativ. Das bedeutet, die Originaldaten wurden verändert.

- Das Ergebnis der Prüfung von Signatur und Zertifikatskette ist negativ. Das bedeutet, die Zertifikatskette konnte zwar vollständig gebildet, jedoch nicht erfolgreich geprüft werden, weil z.B. ein Sperreintrag für einzelne oder alle an der Signatur beteiligten Zertifikate zum Prüfzeitpunkt vorliegt.

Mathematisch korrekt bedeutet, dass die Datei seit dem Signaturzeitpunkt nicht geändert wurde. Außerdem wurde auch die Signatur an sich nicht manipuliert. Empfehlenswert ist es in diesem Fall, eine OCSP Abfrage durchzuführen (siehe Abschnitt 3.3.3) und sich auf diesem Weg bestätigen zu lassen, dass das Signaturzertifikat zum Zeitpunkt der Signaturerstellung gültig und nicht gesperrt war. Dazu wählen Sie das Register mit dem Namen des Signaturinhabers.

3.3.2 Details

Nach Anklicken des Registers mit dem Namen des Signaturinhabers wird Ihnen folgendes Fenster angezeigt.



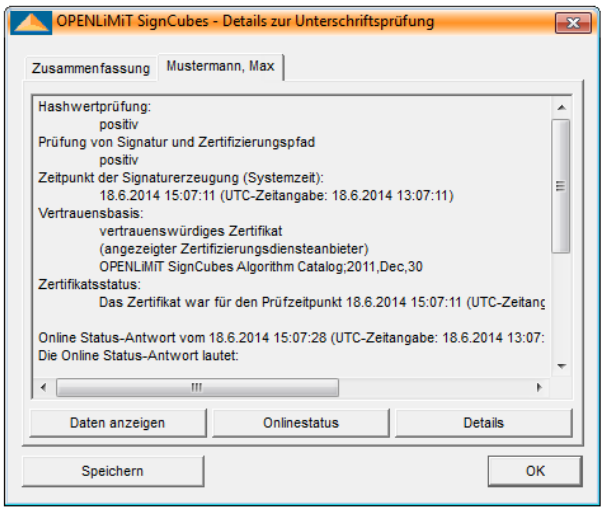
Im Einzelnen erhalten Sie folgende Informationen:

- **Hashwertprüfung:** Hier wird die Integrität der Daten überprüft. Ist die Hashwertprüfung positiv, bedeutet dies, dass die Daten seit dem Signieren nicht verändert wurden. Negativ bedeutet, dass die Daten verändert wurden - in diesem Fall ist die Signatur ungültig. Wird als Zusatzinformation ein Hinweis angezeigt, dass der eingesetzte Hashalgorithmus als ungeeignet eingestuft wird, dann bedeutet das, dass für die Berechnung des Hashwertes ein Hashalgorithmus (z.B. SHA-1) verwendet wurde, der für die Erzeugung qualifizierter Signaturen nicht zulässig ist.
- **Prüfung von Signatur und Zertifizierungspfad:** Hier wird angegeben, ob eine Beschädigung der Signatur vorliegt und ob der Zertifizierungspfad vollständig ist.

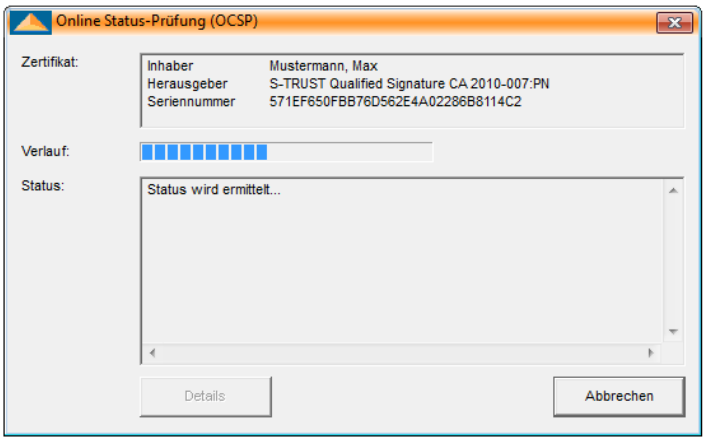
- **Zeitpunkt der Signaturerzeugung (Systemzeit):** Hier wird die Zeit angegeben, die auf dem Rechner zum Zeitpunkt der Signaturerzeugung eingestellt war.
- **Vertrauensbasis:** Hier wird die Vertrauenswürdigkeit des Zertifikats angegeben. Weiterhin wird der für die Signaturprüfung verwendete Algorithmenkatalog angezeigt.
- **Zertifikatsstatus:** Während des Prüfvorgangs wird der Herausgeber des Signaturzertifikats ermittelt und eine OCSP-Anfrage gestellt, um die Gültigkeit des zu untersuchenden Zertifikats zu prüfen. Alternativ zur Benutzung von OCSP kann eine Zertifikatssperrliste für den Prüfvorgang verwendet werden.
- **Aktuelle Zeit als Prüfzeit (Sperrlistenprüfung):** Anhand von Sperrlisten wird geprüft, ob das Zertifikat zum Zeitpunkt der Prüfung gültig war.

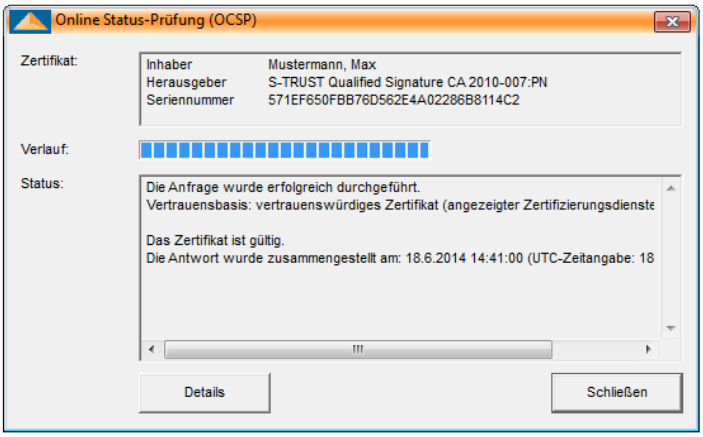
3.3.3 Online Prüfung von Zertifikaten

Neben der Sperrlistenprüfung kann der Status eines Zertifikats auch Online abgefragt werden.



Nach einem Klick auf den Button **[Onlinestatus...]** in dem Fenster **OpenLimit SignCubes - Details zur Unterschriftsprüfung** wird das Fenster Online **Status-Prüfung (OCSP)** geöffnet. Für die Prüfung muss eine Internetverbindung bestehen.



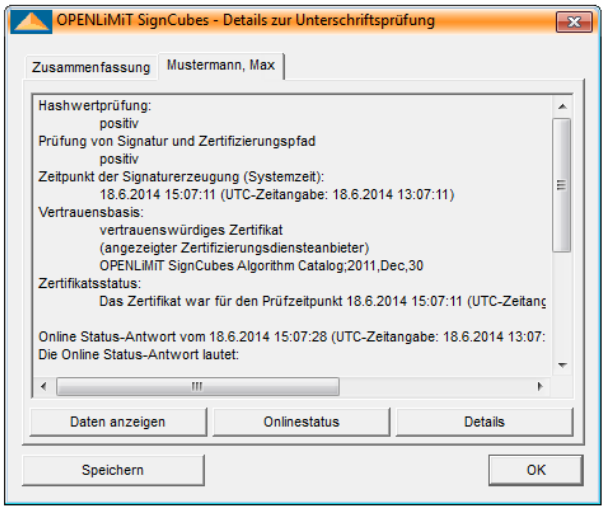


Der Status wird automatisch ermittelt und dann angezeigt. Der Status eines Zertifikats ist entweder gültig, gesperrt oder unbekannt. Das Ergebnis der Online Status-Prüfung wird im normalen Prüfdialog nicht angezeigt. Der Prüfdialog bezieht sich lediglich auf die Sperrlisten/OCSP.

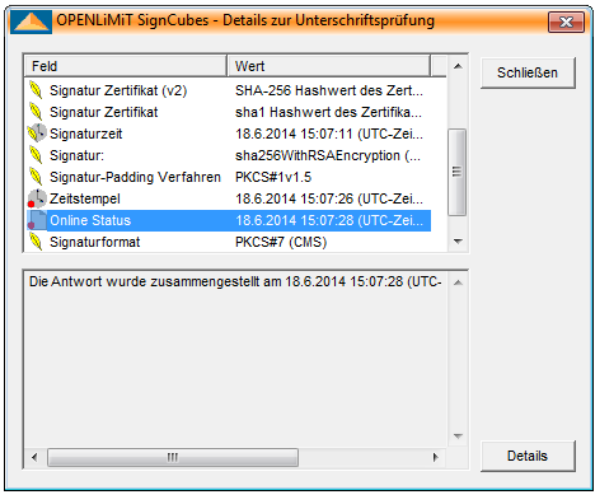
3.3.4 Online Status

Wurde bei der Signaturerstellung der Signatur ein Online Status zugefügt, dann können Sie sich diesen bei der Signaturprüfung ansehen.

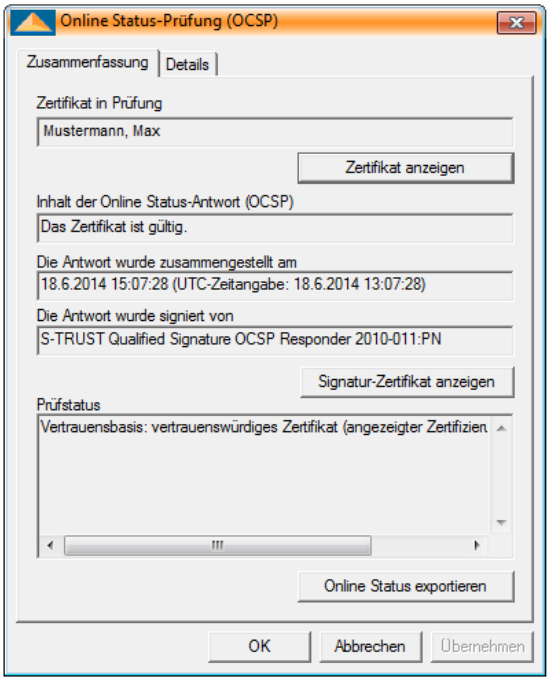
Klicken Sie auf den Button **[Details]**, um die Einzelheiten der Signaturprüfung anzuzeigen.



Wählen Sie dann **[Online Status]** aus und klicken Sie auf **[Details]**, um die Einzelheiten der Online Status Prüfung zum Zeitpunkt der Signaturerzeugung zu sehen.



Klicken Sie auf **[Details]**.



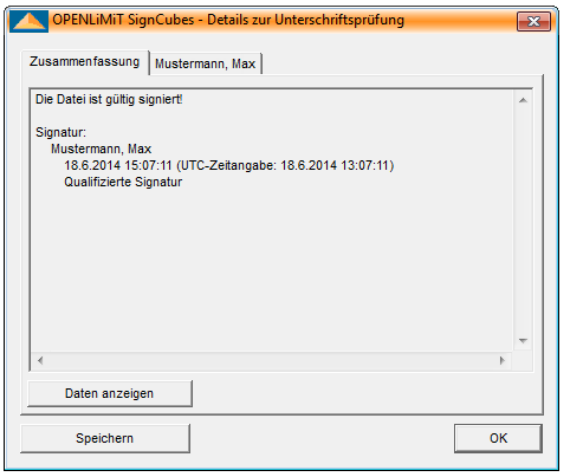
Mit **[Zertifikat anzeigen]** wird das Zertifikat der Person angezeigt, die die Signatur erzeugt hat.

Mit **[Signatur-Zertifikat anzeigen]** wird das Zertifikat der Zertifizierungsstelle angezeigt, die die Online Status Antwort signiert hat.

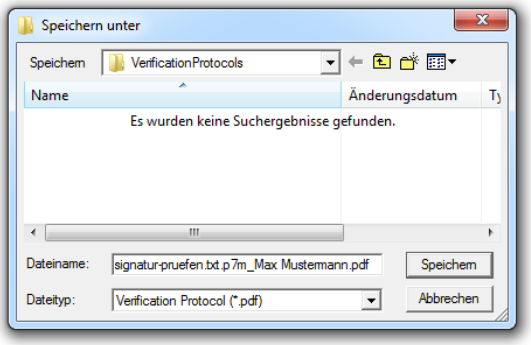
Mit **[Online Status exportieren]** können Sie die Datei als *.ors speichern. Um sich das Ergebnis der Online-Prüfung vollständig ansehen zu können, müssen Sie das dazugehörige Zertifikat in dem gleichen Ordner ablegen.

3.3.5 Erstellen eines Prüfprotokolls

Durch das Anklicken des Buttons **[Speichern]** haben Sie die Möglichkeit, ein Prüfprotokoll zu erzeugen und zu speichern.



Wählen Sie das Verzeichnis und den Dateinamen für das Prüfprotokoll aus. Standardmäßig wird das Protokoll in dem Ordner **C:\Users***angemeldeter User***\Documents\VerificationProtocols** abgespeichert.

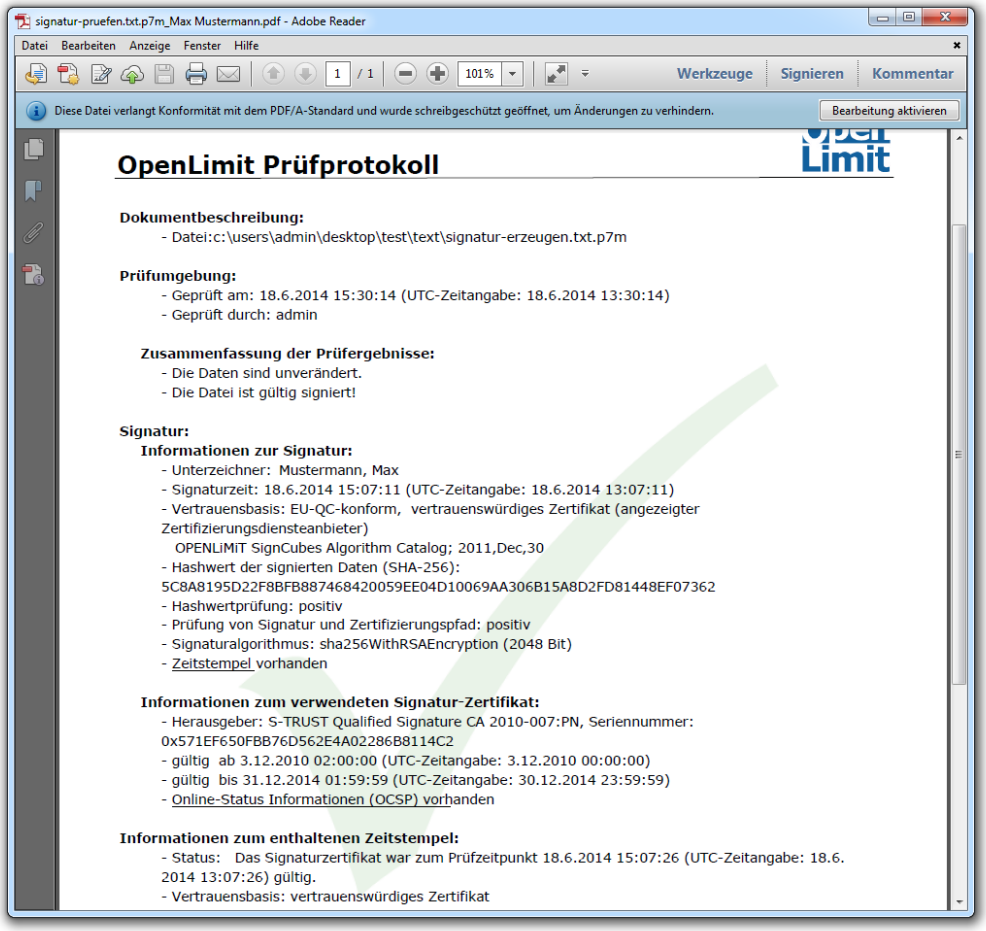


Das Prüfprotokoll enthält folgende Angaben:

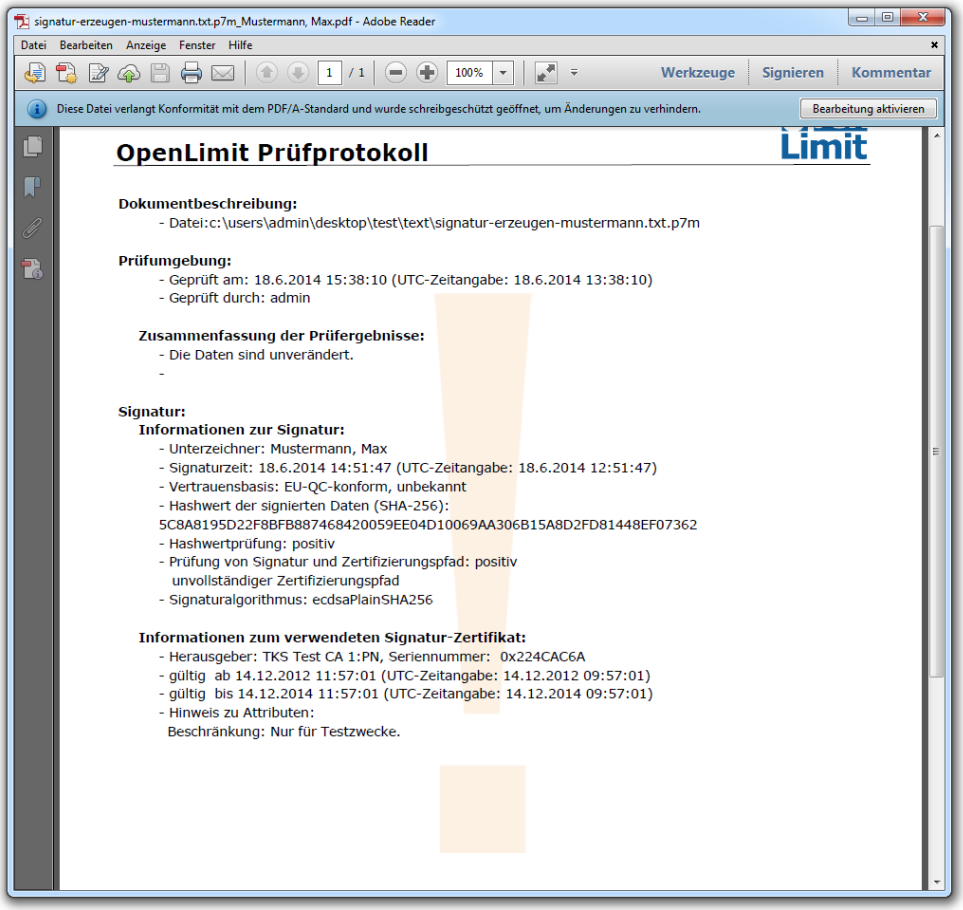
- **Dokumentbeschreibung:** Die Dokumentbeschreibung zeigt den Dateinamen und das temporäre Verzeichnis an, in dem das Prüfprotokoll als Datei zwischengespeichert wird, bevor es entweder abschließend in dem Verzeichnis Eigene Dateien\VerificationProtocols oder in einem durch den Anwender definierten Verzeichnis abgelegt wird.
- **Prüfumgebung:** Die Prüfumgebung weist aus, wann (Datum und Uhrzeit) die Prüfung durchgeführt wurde und durch welchen Nutzer.
- **Zusammenfassung der Prüfergebnisse:** Hier wird das Ergebnis der Hashwertprüfung und die Überprüfung der Zertifizierungskette zusammengefasst dargestellt.

- **Informationen zur Signatur:** An dieser Stelle erhalten Sie weitere Detailinformationen zur Signatur wie den Namen des Unterzeichners, die Signaturzeit, die Vertrauensbasis des Herausgeberzertifikats, den Hashwert, das Ergebnis der Hashwertprüfung und welcher Signaturalgorithmus verwendet wurde.
- **Informationen zum verwendeten Signatur-Zertifikat:** Hier werden die Angaben zum Herausgeberzertifikat, d.h. wer ist der Herausgeber, die Seriennummer des Herausgeberzertifikats und die Gültigkeit ausgewiesen.
- **Online-Status Informationen (OCSP):** Hier wird das Ergebnis der OCSP Anfrage, z.B. die Vertrauensbasis, der Zeitpunkt der Anfrage, der Herausgeber, der Zertifikatsstatus usw., dargestellt.

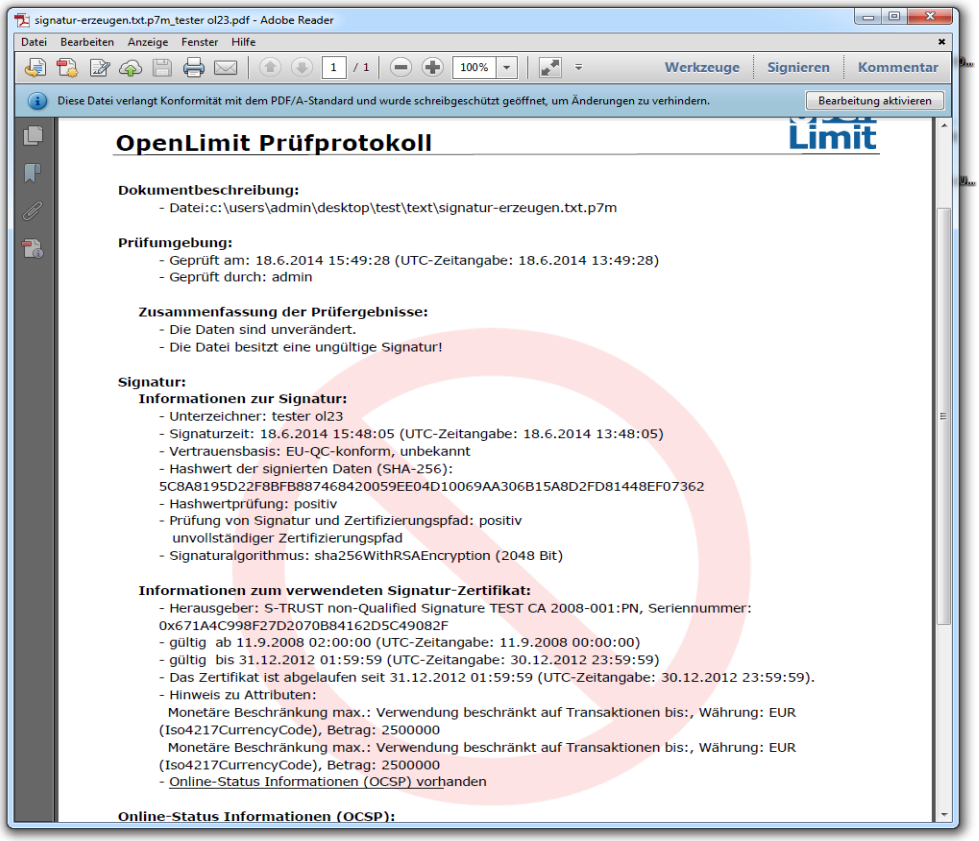
Durch die Symbolik im Hintergrund des Prüfprotokolls (grüner Haken, gelbes Ausrufezeichen, roter Warnkreis) wird das Ergebnis der Prüfung optisch zusätzlich verdeutlicht. Dabei haben die Symbole folgende Bedeutung:



- **Grüner Haken:** Die Signatur wurde gültig geprüft.



- **Oranges Ausrufezeichen:** Es gibt Hinweise darauf, dass die Signatur nicht vollständig geprüft werden konnte, weil z.B. Sperrlisten oder Herausgeberzertifikate fehlten bzw. nicht aktuell waren. In diesem Fall sollten Sie die Aktualisierung der Sperrlisten einschließlich der Vertrauenslisten durchführen und die Signaturverifikation nochmals starten. Weitere Informationen dazu finden Sie in dem Kapitel Sperrlistenaktualisierung.



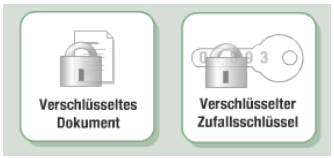
- **Roter Warnkreis:** Dieses Symbol weist daraufhin, dass die Datei eine ungültige Signatur besitzt. In diesem Fall sollten Sie im Detail prüfen, ob die Daten manipuliert wurden, das Zertifikat abgelaufen oder gesperrt ist.

3.4 Verschlüsselung

Die Verschlüsselung schützt vor den Augen Dritter. Sie können jegliche Daten verschlüsseln, egal ob diese auf dem Rechner gespeichert oder ob sie per E-Mail über das Internet gesendet werden. Da die Verschlüsselung aber nicht vor Viren schützt, ist es ratsam, verschlüsselte Daten, die archiviert werden sollen, zusätzlich auf externen Datenträgern zu sichern bzw. nach dem Entschlüsseln auf jeden Fall nach Viren zu prüfen.

Zunächst wird das Dokument mit einem Zufallsschlüssel im 3DES-Verfahren verschlüsselt. Das heißt, das Dokument wird dreimal hintereinander mit 192 Bit verschlüsselt. Der Zufallsschlüssel wird dann mit dem öffentlichen Schlüssel des Empfängers verschlüsselt. Hier kommt die 1024 Bit RSA-Verschlüsselung zum Einsatz.

Man benötigt zum Verschlüsseln also immer den öffentlichen Schlüssel des Empfängers (das können auch mehrere sein). Dieser ist in ein Verschlüsselungszertifikat integriert und kann im Verzeichnisdienst des Trustcenters abgerufen und auf dem Computer installiert werden. Sie können sich auch die Verschlüsselungszertifikate Ihrer Kommunikationspartner per E-Mail schicken lassen. Ihr eigenes Zertifikat können Sie aus der Karte exportieren. Alle installierten Zertifikate werden von der Software automatisch angezeigt. Das verschlüsselte Dokument und der verschlüsselte Zufallsschlüssel werden dann zusammen archiviert oder per E-Mail an die Kommunikationspartner versandt.



In der Praxis ist es empfehlenswert, Daten durch eine Kombination von elektronischer Signatur und Verschlüsselung zu sichern.

3.4.1 Daten verschlüsseln

Die Verschlüsselung von Daten ist nicht gesetzlich geregelt. Dennoch ist es ratsam, Daten zusätzlich zur Signatur zu verschlüsseln, weil dadurch gewährleistet wird, dass nur bestimmte Personen Einblick in die Daten haben.

Wenn Sie Daten verschlüsseln, sollten Sie mindestens 2 Zertifikate verwenden (Ihres und das einer vertrauenswürdigen Person). Wenn Sie Ihre Karte verlieren sollten oder sie auf andere Art unbrauchbar wird, sind die verschlüsselten Daten ansonsten unwiederbringlich verloren. Es gibt keine Kopien Ihres privaten Schlüssels und eine Wiederherstellung ist unmöglich.

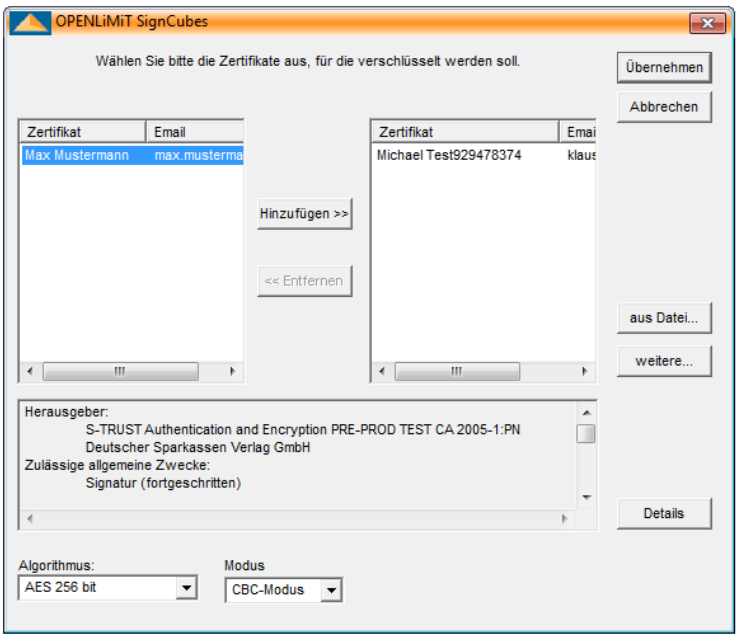
Verschlüsselungszertifikate auswählen

Nachdem Sie auf **[Verschlüsseln]** geklickt haben, erscheint der Dialog zur Auswahl von Verschlüsselungszertifikaten.

Hier werden alle öffentlichen Schlüssel angezeigt, die auf dem Rechner installiert sind. Sollten Sie auf der linken Seite keine Zertifikate außer Ihr eigenes sehen, müssen Sie sich die öffentlichen Schlüssel der Empfänger beschaffen. Sie haben dazu mehrere Möglichkeiten:

- Download oder Installation über den Verzeichnisdienst, dazu erhalten Sie weitere Informationen in dem Abschnitt **Verzeichnisdienst**,
- durch Installation des Schlüssels, den Sie als *.cer-Datei erhalten haben, falls Sie mit diesem Kommunikationspartner mehrfach verschlüsselt kommunizieren wollen; Weitere Informationen finden Sie in dem Abschnitt Zertifikate installieren
- oder durch Einfügen der *.cer-Datei, in dem Sie auf den Button **[aus Datei]** klicken

Nur die Zertifikatsinhaber der ausgewählten Zertifikate können die Datei entschlüsseln. Es ist also ratsam, auch das eigene Zertifikat hinzuzufügen.



Wenn ein Zertifikat selektiert ist, können im unteren Fenster die Informationen dazu angesehen werden.

Nach einem Klick auf **[Hinzufügen]** oder einem Doppelklick auf den Zertifikatsnamen wird das Zertifikat in die rechte Liste kopiert.

Klicken Sie dann auf **[Übernehmen]**, um die Daten für die ausgewählten Zertifikate zu verschlüsseln.

Selektierte Zertifikate können mit Hinzufügen und Entfernen von einem Fenster ins andere verschoben werden. Unter **[Details...]** wird das ausgewählte Zertifikat angezeigt. Um sicher zu gehen, dass das

Zertifikat nicht gesperrt ist, kann nach einem Klick auf Details... der Onlinestatus geprüft werden, wenn die CA das unterstützt.

Sind Sie nicht im Besitz des Partner-Zertifikates, dann haben Sie die Möglichkeit, dieses über den Button **[weitere...]** mit Hilfe der Verzeichnisdienstsuche zu übernehmen oder zu installieren

Einstellung des Verschlüsselungsalgorithmus

Für den Verschlüsselungsalgorithmus sollten Sie nur dann andere Einstellungen vornehmen, wenn es aus Gründen der Kompatibilität mit anderen Programmen unbedingt notwendig ist.

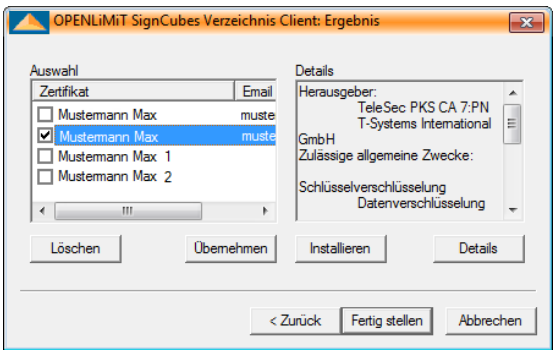
3.4.2 Verschlüsselungszertifikat exportieren

Der OpenLimit SignCubes Security Environment Manager bietet Ihnen die Möglichkeit, Ihr Verschlüsselungszertifikat zu exportieren. Das Zertifikat können Sie dann z.B. per E-Mail an eine andere Person senden, damit diese wiederum Dokumente für Sie verschlüsseln kann.

Weitere Informationen dazu finden Sie in der Online Help im Kapitel „Chipkarten Optionen/Zertifikate exportieren".

3.4.3 Zertifikate anderer Personen installieren

Ein Zertifikat aus dem Verzeichnisdienst installieren Sie, indem Sie auf den Button **[Installieren]** im Ergebnisdialog klicken. Das Zertifikat erscheint beim nächsten Verschlüsseln automatisch im Zertifikatsauswahldialog.



Wenn Sie ein Zertifikat auf anderem Weg erhalten, z.B. per E-Mail, liegt es als Datei vor. Sie müssen es über den Zertifikatsdialog von Windows installieren.

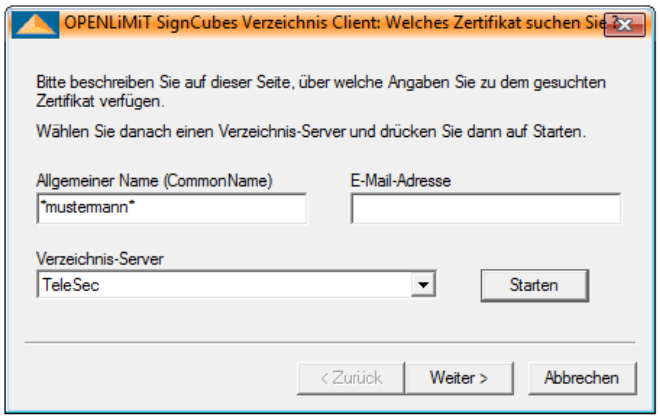
Zertifikate in den Microsoft Zertifikatsspeicher installieren

- Doppelklicken Sie das Zertifikat im Windows Explorer.
- Klicken Sie im Fenster **Zertifikat** auf den Button **[Zertifikat installieren...]** und folgen Sie den Anweisungen

- Nach dem Startdialog folgt mit einem Klick auf **[Weiter]** der Zertifikatsspeicherdialog.
- Wählen Sie: Alle Zertifikate in folgendem Speicher speichern.
- Klicken Sie auf **[Durchsuchen...]**
- Wählen Sie den Ordner **Andere Personen** und bestätigen Sie mit **[OK]**.
- Klicken Sie im Assistenten auf **[Weiter]**.
- und anschließend auf **[Fertig stellen]**.
- Das Zertifikat erscheint beim nächsten Verschlüsseln automatisch im Zertifikatsauswahl Dialog.

3.4.4 Verzeichnisdienst

Nach einem Klick auf **[weitere...]** wird der Verzeichnis Client geöffnet.



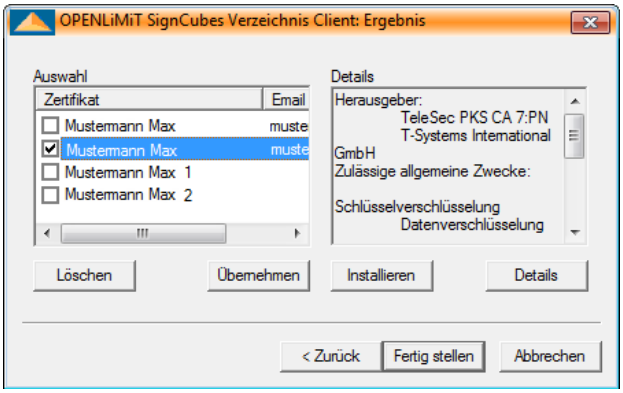
Für die Suche können Sie Wildcards (*) benutzen. Das sind Platzhalter, die man für unbekannte Buchstaben platzieren kann. Wenn Sie dies nicht tun, müssen Sie die exakte Schreibweise des gesuchten Namens kennen. Geben Sie am besten den Nachnamen zwischen Wildcards ein: z.B. *Daneller*.

Zertifikat suchen

- Tragen Sie den oder die Suchbegriffe in die Felder ein.
- Wählen Sie den Verzeichnisdienst der CA, die das Zertifikat herausgegeben hat.
- Klicken Sie im Anschluss auf **[Starten]**.

Wenn Sie eine Fehlermeldung erhalten, dass die zulässige Größe überschritten ist, dann haben Sie zu viele Suchergebnisse erhalten. Diese Funktion dient dem Datenschutz, so dass nicht einfach mit einer * * -Suche alle Zertifikate gefunden werden können. Geben Sie weitere Buchstaben in den Suchbegriff ein.

Im Ergebnisdialog werden alle gefundenen Zertifikate angezeigt.



Zertifikate übernehmen

- Mit einem Klick auf den Namen wird rechts die Zertifikatsinformation angezeigt.
- Über den Button **[Details]** kommt man zur Zertifikatsanzeige, wo man sich noch einmal die Einzelheiten ansehen kann. Die meisten CAs nehmen gesperrte und ungültige Zertifikate aus dem Verzeichnisdienst, so dass sich eine Statusprüfung erübrigt, wenn man hier ein Zertifikat gefunden hat.
- Damit das Zertifikat auf dem Rechner bei jeder Verschlüsselung automatisch angezeigt wird, kann es installiert werden. Dies sollten Sie für Zertifikate tun, die Sie oft benutzen.
- Haken Sie die Checkbox vor dem Namen der Zertifikate an, die für die Verschlüsselung übernommen werden sollen.
- Klicken Sie auf **[Übernehmen]**.
- Die Zertifikate erscheinen dann im Zertifikatsauswahl Dialog (Verschlüsseln) auf der rechten Seite.

3.5 Entschlüsselung

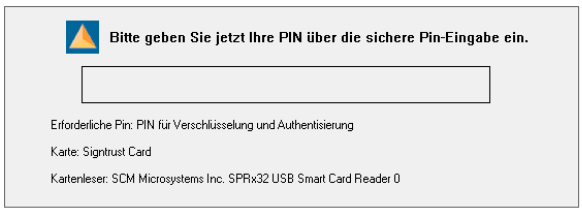
Um das Dokument wieder entschlüsseln zu können, wird der Zufallsschlüssel im Klartext benötigt. Er kann nur mit dem privaten Schlüssel entschlüsselt werden. Dazu braucht der Benutzer die Karte mit dem, zu dem öffentlichen Schlüssel zugehörigen privaten Schlüssel und der PIN.

Ist der Zufallsschlüssel entschlüsselt, kann auch das gesamte Dokument entschlüsselt werden. Auch diese Abläufe übernimmt die Software automatisch.

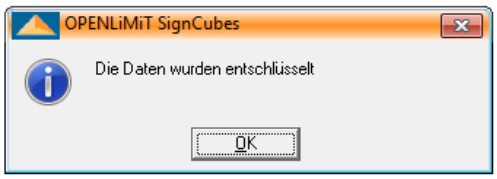
Durch dieses Verfahren ist gesichert, dass nur der Karteninhaber mit seiner PIN das Dokument entschlüsseln und lesen kann. Die Daten können auch für mehrere Zertifikate verschlüsselt werden. Wir empfehlen grundsätzlich, alle Daten, mindesten mit zwei öffentlichen Schlüsseln, für eine andere vertrauenswürdige Person und sich selbst, zu verschlüsseln. Bei Daten, die versendet werden, empfiehlt es sich das eigene Zertifikat und das des Empfängers. Wenn die eigene Karte verloren geht, oder möglicherweise aus anderen Gründen nicht mehr verwendbar ist, können die Daten immer noch mit der zweiten Karte (der des Empfängers oder der vertrauenswürdigen Person) entschlüsselt werden.

3.5.1 Daten entschlüsseln

Zum Entschlüsseln wird der zu dem öffentlichen Schlüssel zugehörige private Schlüssel benötigt. Aus diesem Grund muss zum Entschlüsseln die globale PIN eingegeben werden.



Es erscheint ein Fenster mit der Meldung, dass die Datei entschlüsselt wurde. Klicken Sie auf **[OK]**.



Danach sollten die Daten wieder im Klartext vorliegen. Um viele Dateien hintereinander ohne ständige PIN-Eingabe zu entschlüsseln, können Sie die Karte auch „öffnen“. Weitere Informationen dazu finden Sie in dem Abschnitt PIN-Abfrage.

4 Die Oberfläche der OpenLimit SignCubes Shellextension

Die OpenLimit SignCubes Shellextension ermöglicht das Erzeugen einer Signatur, eines Zeitstempels und die Verschlüsselung direkt im Windows Explorer. Darüber hinaus sind das Prüfen von Signaturen und die Entschlüsselung integriert. Wenn Sie eine Datei mit der **[rechten Maustaste]** anklicken, finden Sie im Kontextmenü den Punkt **[OpenLimit].**

Wählen Sie diesen aus, erhalten Sie in Abhängigkeit von der ausgewählten Dateistruktur verschiedene Funktionen angeboten. Weitere Informationen erhalten Sie in den nachfolgenden Abschnitten.

4.1 Shellextension Menü

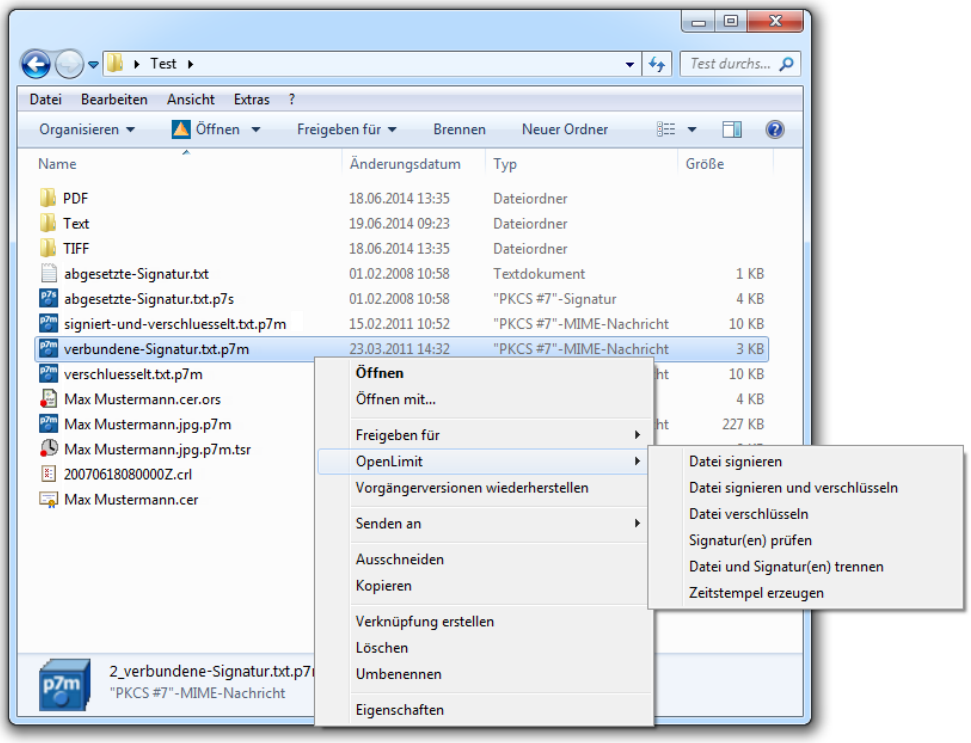
Wenn Sie eine Datei im Windows Explorer mit der **[rechten Maustaste]** anklicken, öffnet sich das Kontextmenü mit dem Menüpunkt **[OpenLimit SignCubes].** Unter diesem finden Sie in der Regel die Punkte:

- Datei signieren
- Datei verschlüsseln
- Datei signieren und verschlüsseln
- Zeitstempel erzeugen

Weitere Punkte, wie z.B.

- Eingebetteten Zeitstempel erzeugen (bei Auswahl einer PDF-Datei)
- Signatur(en) prüfen
- Datei entschlüsseln
- Datei und Signatur(en) trennen
- Datei und Signaturen verbinden
- Zertifikat anzeigen
- Online Status anzeigen
- Zeitstempel erzeugen
- Sperrlisten anzeigen

erscheinen, wenn es sich um bereits signierte oder verschlüsselte Dateien bzw. einen Zeitstempel oder eine Online Status-Datei handelt. Die Funktionen, die durch diese Befehle angestoßen werden, sind unter Arbeitsabläufe im Einzelnen erklärt.

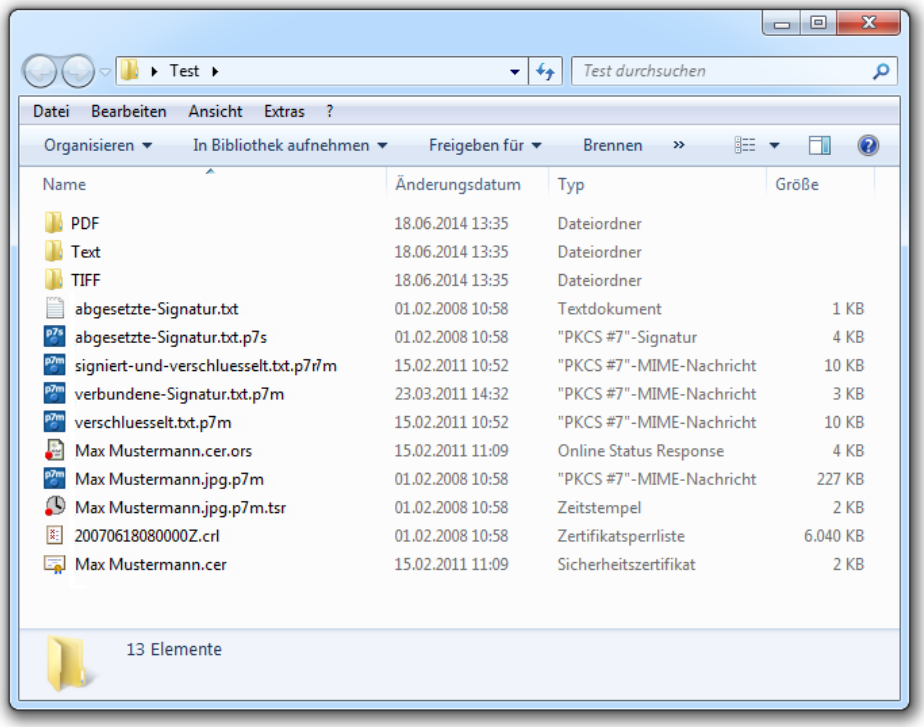


4.2 Dateien und Icons im Windows Explorer

Mit OpenLimit SignCubes lassen sich verschiedene Dateiformate erzeugen. Diese erkennt man im Explorer auch an Ihren Icons.

- **p7m Dateien:** Verschlüsselte Dateien oder Dateien, die eine Signatur beinhalten, bekommen ein blaues Tresor-Icon mit der Aufschrift p7m.
- **p7s Dateien:** Abgesetzte Signaturen, die durch ihren Dateinamen mit der Ausgangsdatei logisch verknüpft sind, bekommen ein blaues Tresor-Icon mit der Aufschrift p7s.
- **ors-Dateien:** Online Status Response Dateien, die durch das Exportieren von OCSP Antworten entstehen, bekommen ein Zertifikats-Icon mit einem roten Siegel.
- **tsr-Dateien:** Zeitstempel Dateien, die durch ihren Dateinamen mit der Ausgangsdatei logisch verknüpft sind, bekommen ein Uhr-Icon mit einem roten Siegel.

Allerdings werden diese Dateien in den neueren Betriebssystemen als verborgene Dateien oft nicht angezeigt. Um sie sichtbar zu machen, muss man unter den Ordneroptionen des Windows Explorers (Menü Extras - Ordneroptionen - Reiter Ansicht) unter versteckte Dateien und Ordner die Option alle Dateien und Ordner anzeigen aktivieren und Erweiterungen bei bekannten Dateitypen ausblenden deaktivieren.



Weitere Informationen zu den Dateien finden Sie im Abschnitt 2 Dateiformate.

5 Adobe Plugin

Das Adobe Plugin ermöglicht die Signatur direkt unter Adobe Acrobat Reader ab Version 7.0.8 und Adobe Acrobat 7.0. Wurden PDF-Formulare vom Herausgeber mit zusätzlichen Rechten versehen (Adobe Formular Server Lösungen), lassen sich diese Formulare auch im Adobe Reader ab Version 7.0.8 signieren. Zudem können digitale Signaturen in einem PDF-Formular geprüft werden.

Hinweis: Ein benötigtes Adobe Plug-In wird bei der Installation automatisch in das entsprechende Verzeichnis des Adobe Reader bzw. Adobe Acrobat kopiert. Sollte zum Zeitpunkt der Installation kein Adobe Reader oder Adobe Acrobat auf dem System vorhanden sein, können Sie das Plug-In nachträglich installieren. Starten Sie dazu den UpdateCheck über das Start/Alle Programme/OpenLimit/OpenLimit UpdateCheck oder Apps/OpenLimit/OpenLimit UpdateCheck und folgen Sie den Anweisungen.

5.1 Adobe Plugin Grundeinstellungen

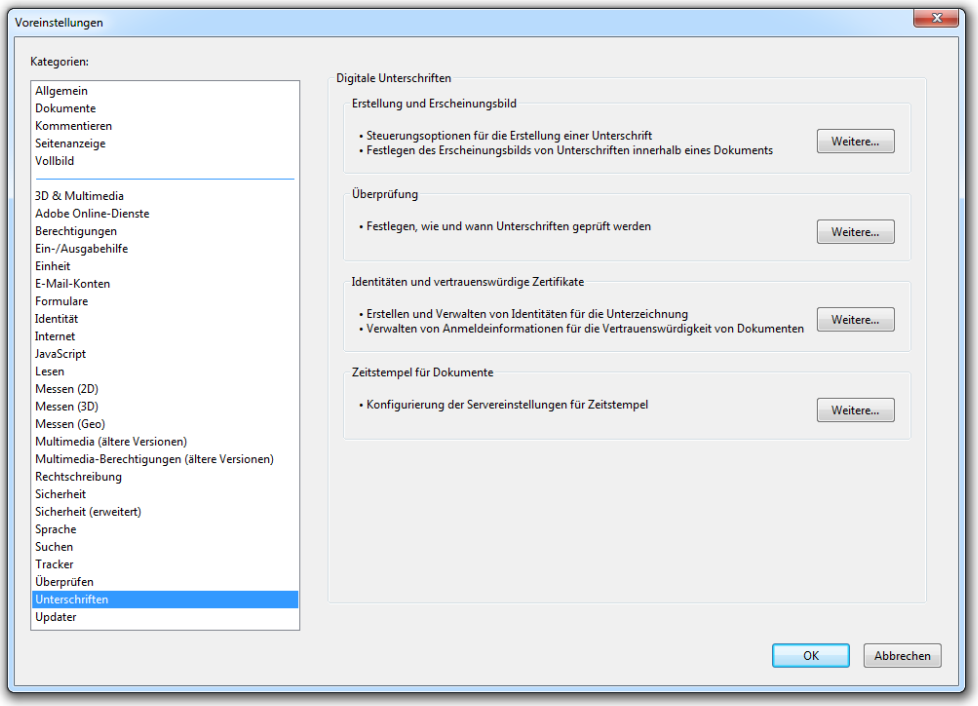
Grundeinstellungen festlegen

Der hier beschriebene Ablauf bezieht sich auf das Produkt Adobe Reader Version 11.0.6. Die Beschreibung erfolgt beispielhaft. Weitere Informationen zu aktuellen Versionen der Adobe Produkte finden Sie unter auf der OpenLimit FAQ Seite unter

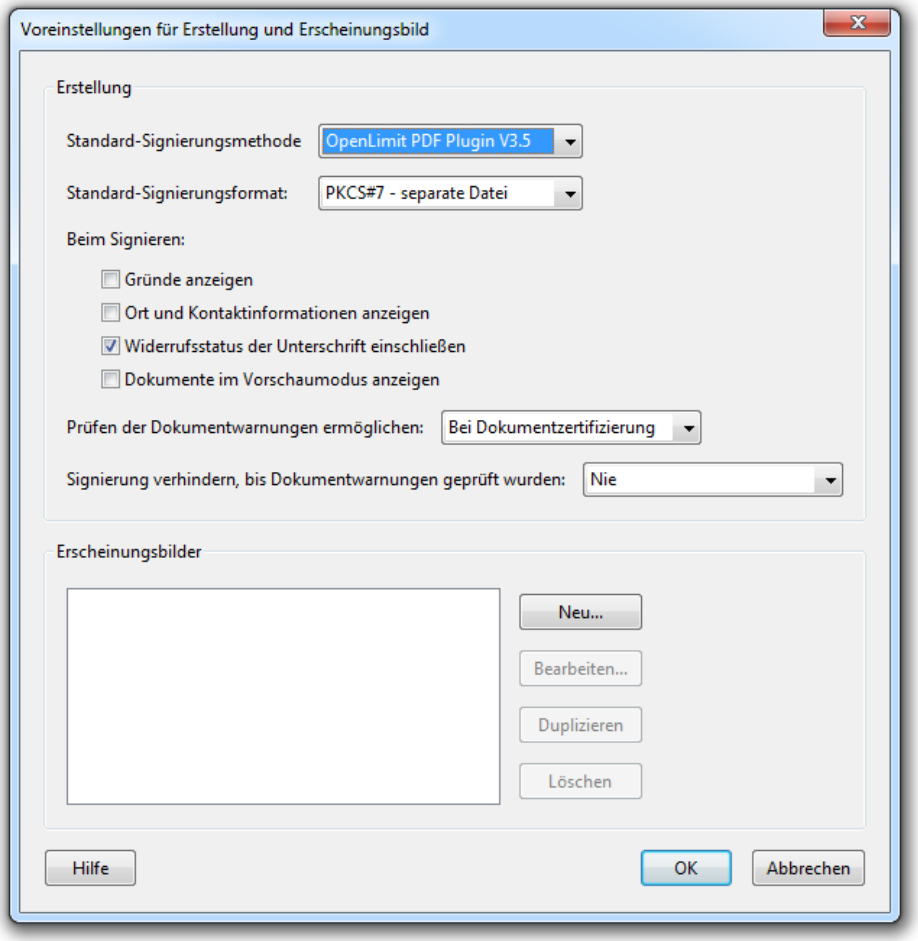
- https://www.openlimit.com/FAQv2/

in der Rubrik Adobe Plugin.

- Öffnen Sie den Adobe Reader.
- Über das Bearbeiten-Menü kommen Sie zu dem Menüpunkt **[Voreinstellungen...]**

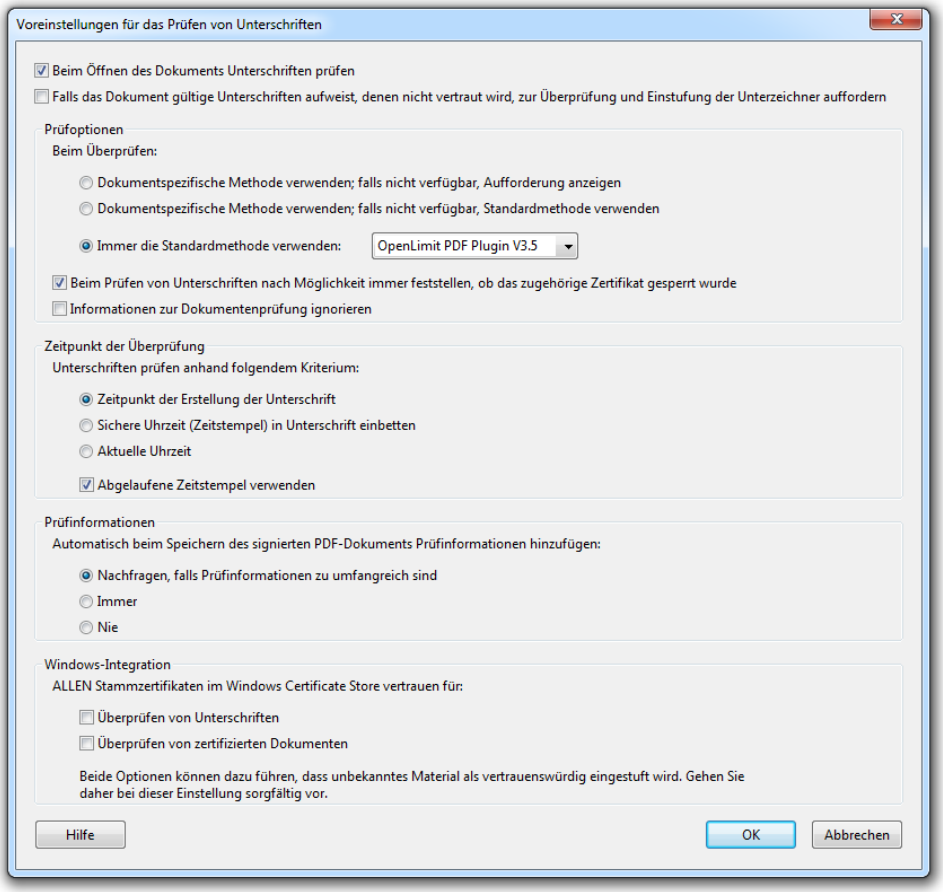


- Wählen Sie im linken Bereich **[Unterschriften]** aus.
- Klicken Sie auf den **[Weitere...]** Button unter der Rubrik Digitale Unterschriften



- Wählen Sie als Standard-Signierungsmethode das OpenLimit PDF Plugin V3.5 aus und bestätigen Sie die Auswahl über **[OK]**.

Für die Einstellung zur Signaturprüfung klicken Sie unter der Rubrik Überprüfung auf den Button **[Weitere...]** und wählen als Standardmethode das OpenLimit PDF Plugin V3.5 aus.



- Mit **[OK]** werden die Einstellungen gespeichert.

5.1.1 PDF-Dokument mit Adobe signieren

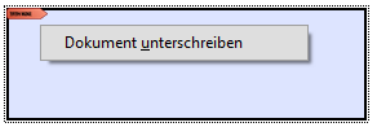
Wenn ein PDF-Dokument oder PDF-Formular ein oder mehrere Felder für digitale Signaturen enthält, so können Sie mit dem Adobe Plugin eine qualifizierte digitale Signatur direkt in diesem PDF erstellen und dieses anschließend speichern.

Um ein solches PDF mit dem Adobe Reader zu signieren, muss dieses mit zusätzlichen Rechten versehen worden sein (Adobe Formular Server Lösungen). Um ein PDF mit Adobe Acrobat zu signieren, reicht es aus, wenn das Signaturfeld mit Adobe Acrobat erstellt wurde. Um ein Signaturfeld mit Adobe Acrobat selbst zu erstellen, lesen Sie bitte in der Adobe Acrobat Hilfe nach.

So signieren Sie ein PDF-Dokument

- Öffnen Sie das Dokument.

Das PDF-Dokument enthält ein oder mehrere Signatur-Felder. Ein Signaturfeld erkennen Sie am roten Pfeil links oben im Feld.



- Stecken Sie Ihre Smartcard in den Kartenleser und warten Sie, bis diese erkannt ist (bis das Chip-Symbol in der Taskleiste gelb ist).
- Klicken Sie das entsprechende Signaturfeld an.

Anschließend öffnet sich das Signaturanforderungsfenster. Weitere Informationen finden Sie in dem Abschnitt **[Signatur erzeugen]**.

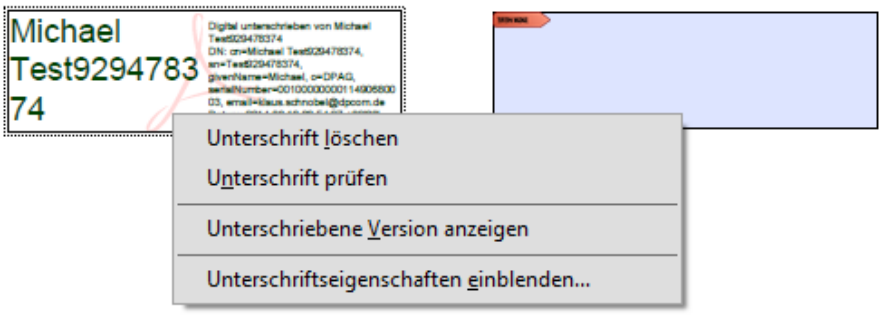
5.1.2 Signatur im PDF mit Adobe prüfen

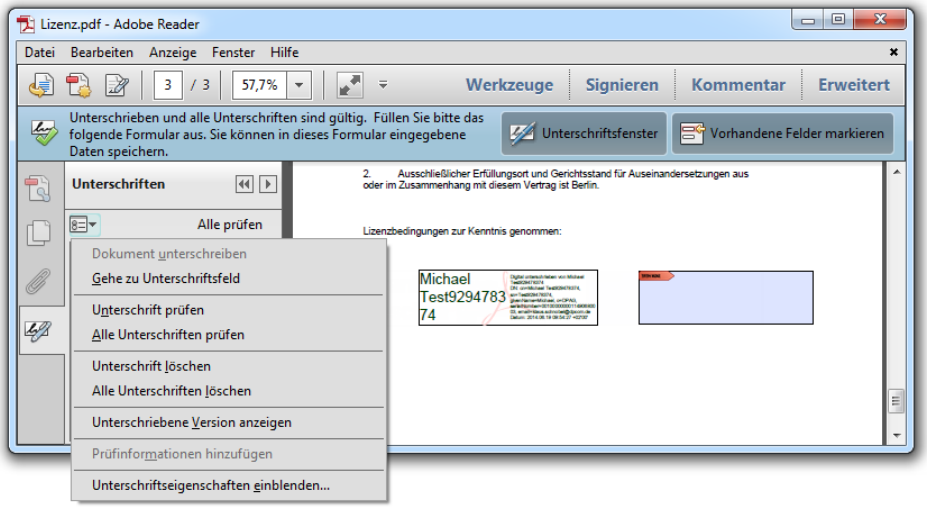
PDF-Dokumente können Signaturen enthalten, die in einem extra dafür vorgesehenen Signaturfeld integriert sind, oder Signaturen, die in das PDF-Dokument eingebettet sind, jedoch nicht in einem Signaturfeld vorliegen. In diesem Fall handelt es sich um sogenannte „eingebettete“ Signaturen.

Signaturen in Unterschriftsfeldern prüfen

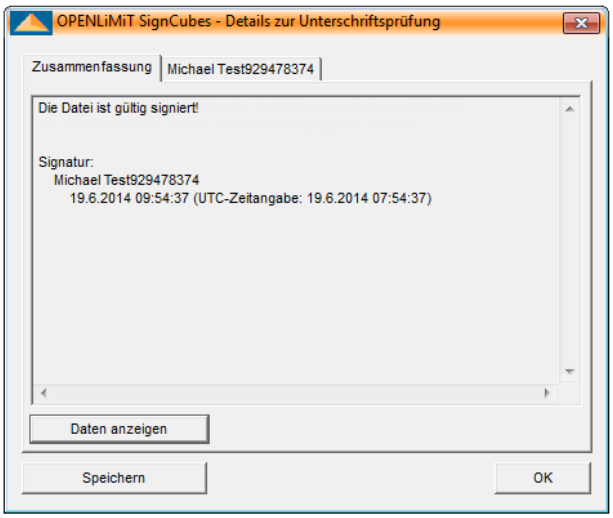
Enthält ein PDF-Dokument bereits eine digitale Signatur in einem dafür vorgesehenen Signaturfeld, so können Sie mit dem Adobe Reader oder Adobe Acrobat diese Signatur prüfen. Die Signaturprüfung wird mit den Einstellungen vorgenommen, die Sie unter Adobe Acrobat oder Adobe Reader festgelegt haben. Weitere Informationen dazu finden Sie in dem Abschnitt **Adobe Plugin Grundeinstellungen**.

Öffnen Sie das PDF-Dokument und klicken Sie auf ein Unterschriftsfeld, das bereits eine Signatur enthält.





Wenn Sie als Standardmethode zum Überprüfen von Unterschriften das „OpenLimit SignCubes PDF Plugin“ ausgewählt haben, so erscheint folgender Dialog:



In der Zusammenfassung steht das Ergebnis der Signaturprüfung. Ein Beispiel für ein Prüfergebnis ist z.B.:

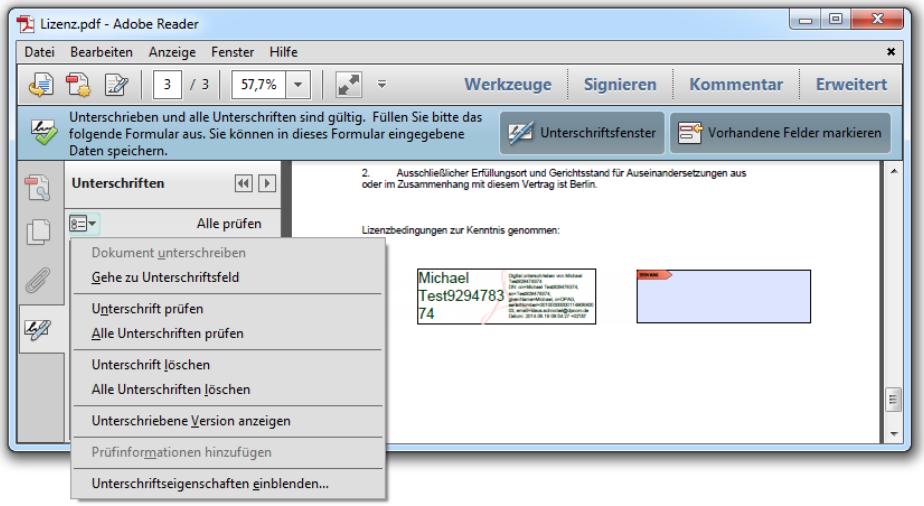
- Die Datei ist gültig signiert. oder
- Die Signatur ist mathematisch korrekt.

Für genauere Informationen lesen Sie bitte in den Abschnitten Signaturverifikation bzw. Signaturen prüfen nach.

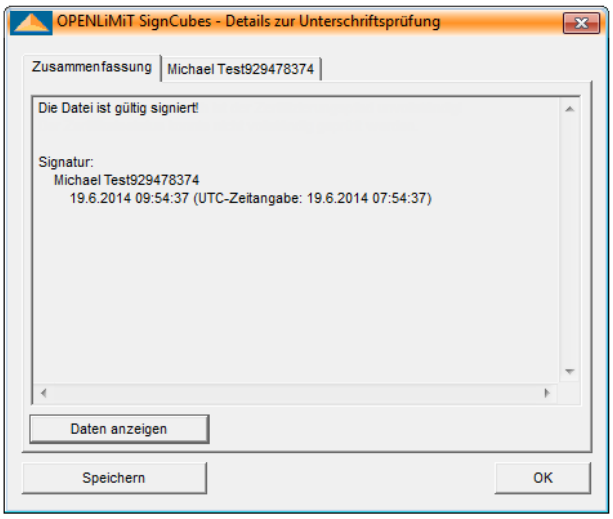
Unsichtbare Signaturen prüfen

Enthält ein PDF-Dokument eine unsichtbare digitale Signatur, so können Sie mit Adobe Reader oder Adobe Acrobat diese Signatur prüfen. Die Signaturprüfung wird mit den Einstellungen vorgenommen, die Sie unter Adobe Acrobat oder Adobe Reader festgelegt haben.

- Öffnen Sie das PDF-Dokument und klicken Sie dann links auf den Reiter **[Unterschriften]**, um alle Unterschriften des Dokuments anzusehen.
- Wählen Sie jetzt eine Unterschrift aus, klicken Sie dann auf **[Optionen]** und wählen Sie Unterschrift prüfen.



Wenn Sie als Standardmethode zum Überprüfen von Unterschriften das „OpenLimit PDF Plugin V3.5“ ausgewählt haben, so erscheint folgender Dialog:



Detaillierte Informationen zu den Ergebnissen der Signaturprüfung finden Sie in dem Abschnitt **Signaturen prüfen**.

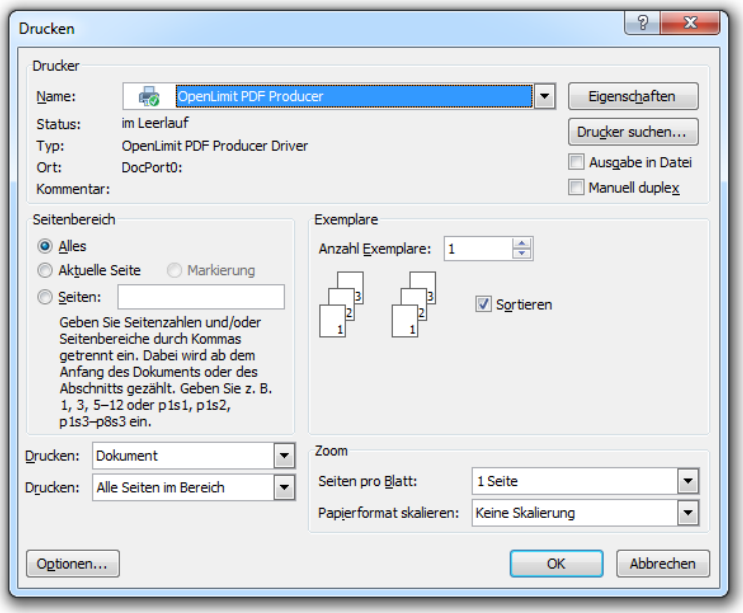
6 Der OpenLimit PDF Producer

OpenLimit CC Sign 2.8 bietet Ihnen mit dem OpenLimit PDF Producer die Möglichkeit, aus anderen Programmen heraus wie z.B. Microsoft Word Daten an die sichere Anzeigeeinheit, den OpenLimit Viewer auszugeben. Die übertragenen Daten werden über den OpenLimit PDF Producer in eine PDF-Datei konvertiert. Die Ausgabe über den OpenLimit PDF Producer ist mit jedem auf Ihrem System druckbaren Dokument möglich.

Visualisieren

Drucken Sie die Datei in dem Programm aus, in dem sie erstellt wurde. Normalerweise geht das über den Befehl **[Datei – Drucken].**

Wählen Sie den **[OpenLimit PDF Producer]** für die Konvertierung als PDF-Datei und bestätigen Sie mit **[OK]**.



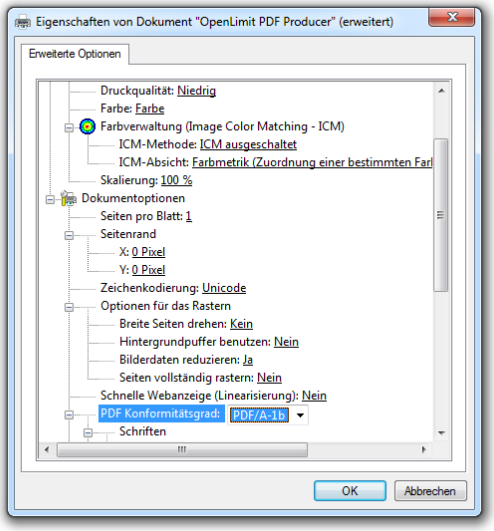
Die konvertierte Datei wird standardmäßig in dem Ordner **[Eigene Dateien\PDFOutput]** abgespeichert. Unter dem Betriebssystem Microsoft Vista finden Sie die Datei in dem Ordner **[Dokumente\PDFOutput]**.

Der Dateiname ist mit dem Dateinamen des Originals identisch, mit Ausnahme der Extension (pdf).

Daraufhin öffnet sich die Darstellung im OpenLimit Viewer. Sollte es lange dauern, bis Ihre Datei im OpenLimit Viewer dargestellt wird, liegt es möglicherweise daran, dass die gewählten Eigenschaften des Druckers mit einer zu hohen Auflösung eingestellt sind.

6.1 Eigenschaften des OpenLimit PDF Producer

Nach Auswahl des OpenLimit PDF Producer und Anklicken des Buttons Eigenschaften haben Sie Möglichkeit die Standardeinstellungen des Druckers zu verändern.



Über das Menü PDF Compliance Level haben Sie die Möglichkeit die PDF-Version einschließlich PDF/A Konformität auszuwählen.

7 Arbeiten mit der Zertifikatsregistrierung oder dem CSP

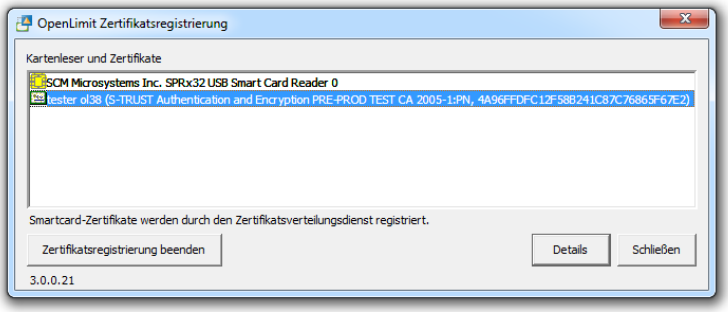
Zur Unterstützung der Erzeugung von E-Mail Signaturen, der Verschlüsselung unter Outlook und die SSL-Authentisierung im Internetexplorer kann sowohl die OpenLimit Zertifikatsregistrierung als auch der Cryptographic Service Provider (CSP) zum Einsatz kommen. Der Anwender hat die Möglichkeit, zwischen beiden Komponenten umzuschalten:

7.1 Die Zertifikatsregistrierung

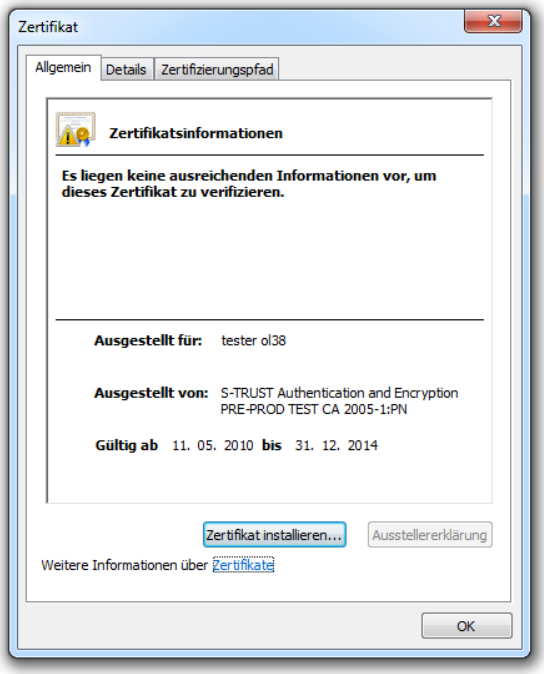
Die OpenLimit Zertifikatsregistrierung ist eine zusätzliche Komponente, die entweder mit OpenLimit CC Sign Version 2.8 installiert oder zusätzlich bereitgestellt werden kann.

Die OpenLimit Zertifikatsregistrierung funktioniert als Windows-Dienst, der ein Zertifikat auf einer Signaturkarte nach dem Erkennen durch die OpenLimit CC Sign Version 2.8 in dem Windows Zertifikatsspeicher unter der Rubrik „Eigene Zertifikate“ registriert. Nach dem Entfernen der Signaturkarte im Kartenleser wird das Zertifikat im Windows Zertifikatsspeicher gelöscht. Damit steht dieses Zertifikat auch für andere Anwendungen über OpenLimit CC Sign hinaus zur Verfügung.
Die OpenLimit Zertifikatsregistrierung wird nicht automatisch gestartet, sondern muss über **[Start/Alle Programme/OpenLimit/Zertifikatsregistrierung oder Apps/OpenLimit/Zertifikatsregistrierung]** geöffnet werden. Anschließend erscheint das folgende Icon in der Taskleiste:

Nach Anklicken des Icons öffnet sich das folgende Fenster, in dem der bzw. die Kartenleser und die einsatzbereiten Zertifikate angezeigt werden.



Über den Button **[Schließen]** wird die Anzeige wieder minimiert. Wenn Sie ein Zertifikat ausgewählt haben und den Button **[Details]** anklicken, wird das Fenster des Windows Zertifikatsmanagers geöffnet und die Informationen zum Zertifikat angezeigt.



Über den Button **[Zertifikatsregistrierung beenden]** wird die Komponente beendet und die Zertifikate werden aus dem Windows Zertifikatsspeicher gelöscht.

Hinweis: Während der Erzeugung einer Signatur einer E-Mail als auch bei der Entschlüsselung einer E-Mail werden Sie aufgefordert, die PIN zu dem fortgeschrittenen Zertifikat einzugeben. Erfolgt der Zugriff auf die Zertifikate über die OpenLimit Zertifikatsregistrierung, wird die PIN für weitere Vorgänge offen gehalten, obwohl ein gelbes Chipsymbol (statt ein rotes) angezeigt wird. Um Missbrauch Ihrer Zertifikate zu verhindern, ist es notwendig, beim Verlassen des Arbeitsplatzes unbedingt die Karte aus dem Kartenleser zu ziehen.

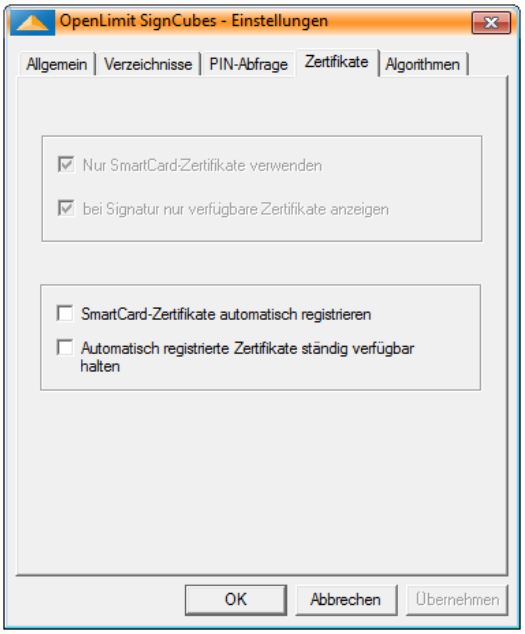
7.2 Der CSP

Der Cryptographic Service Provider (CSP) ist Bestandteil der Software OpenLimit CC Sign 2.8 und organisiert den Zugriff auf die Zertifikate über die OpenLimit Komponenten.

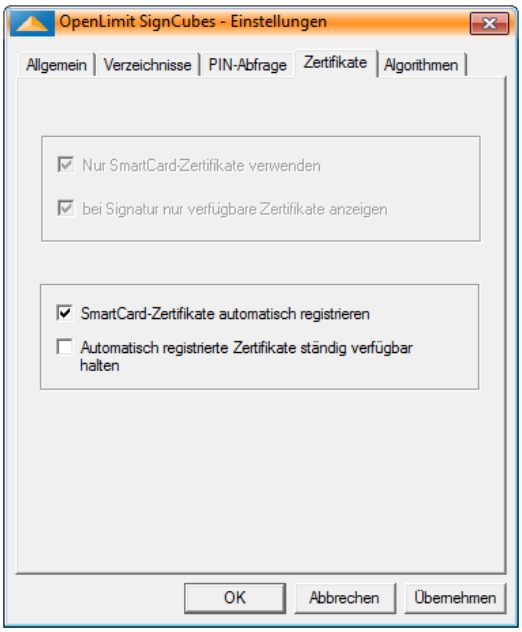
7.3 Umschalten zwischen der Zertifikatsregistrierung und dem CSP

Standardmäßig wird mit der Installation von OpenLimit CC Sign 2.8 die Zusatzkomponente OpenLimit Zertifikatsregistrierung verwendet. Das Umschalten auf die Verwendung des CSP erfolgt wie nachfolgend beschrieben:

- Klicken Sie auf das OpenLimit Icon in der Taskleiste, wählen das Menü Einstellungen und anschließend das Register Zertifikate aus:



- Setzen Sie den Haken für **[Smartcard- Zertifikate automatisch registrieren]** und Beenden die Einstellung über den Button **[Übernehmen]**.



- Da die Einstellungen erst mit Neustart der OpenLimit Software zum Einsatz kommen, beenden Sie bitte OpenLimit durch Anklicken des OpenLimit Icons in der Taskleiste und Klick auf **[Beenden]**. Anschließend starten sie den OpenLimit Manager neu.

8 E-Mail Clients

Die Software OpenLimit CC Sign 2.8 unterstützt das Signieren und Verschlüsseln von E-Mails in verschiedenen E-Mail Programmen. Die Arbeit mit den verschiedenen E-Mail Programmen setzt zunächst voraus, dass das E-Mail Programm ordnungsgemäß installiert ist.

8.1 Microsoft Outlook

Beim Einsatz von Outlook ist zu beachten, dass das E-Mail Konto mit der E-Mail Adresse Ihres Zertifikats übereinstimmt, d.h. damit Sie mit Ihrer Signaturkarte eine E-Mail signieren können, muss die E-Mailadresse im Zertifikat gleich der E-Mail-Adresse in Ihrem E-Mail-Konto sein.

Die Informationen der E-Mail Adresse im Zertifikat können Sie sich wie folgt anzeigen lassen:

- klicken Sie auf das gelbe Chip-Symbol in der **[Taskleiste / Eigenschaften / Zertifikate]**
- klicken Sie das fortgeschrittene Zertifikat und dann den Button **[Details]** an
- unter dem Reiter **[Details]** wird Ihnen die im Zertifikat integrierte E-Mail-Adresse angezeigt
- zu dieser E-Mail-Adresse muss es in Outlook ein E-Mail-Konto geben

Im nächsten Schritt sollten Sie prüfen, ob die E-Mailadresse im Zertifikat mit der E-Mail-Adresse in Ihrem E-Mail-Konto übereinstimmt. Daran anschließend müssen Sie über das Outlook Hauptmenü die notwendigen Sicherheitseinstellungen für das Erzeugen einer Signatur bzw. für die Verschlüsselung vornehmen.

Weitere Informationen zu aktuellen Versionen der E-Mail Clients finden Sie auf der OpenLimit FAQ Seite unter

- https://www.openlimit.com/FAQv2/

unter der Kategorie E-Mail Clients/Outlook.

8.2 Thunderbird

Falls Sie Thunderbird als E-Mail Client verwenden, sind für die E-Mail Signatur und Verschlüsselung die folgenden Einstellungen vorzunehmen:

- Laden des P11-Treibers

Über das Thunderbird-Hauptmenü **[Extras/Einstellungen/Erweitert/Reiter „Zertifikate"/Kryptographie-Module]** müssen Sie unseren OpenLimit P11-Treiber (siqp11.dll) in den Kryptographie-Manager laden. Wählen Sie die Datei „siqp11.dll" im Verzeichnis **C:\Program Files (x86)\OPENLiMiT** aus und bestätigen Sie mit **[OK]**.

Im Anschluss wird ein „Neues PKCS#11 Modul“ mit dem Pfad unseres P11-Treibers angezeigt.

- Kontrolle der Vertrauensstellung der Zertifikatsaussteller

Bitte stecken Sie die Signaturkarte in den Kartenleser und warten Sie bis das Chipsymbol in der Taskleiste gelb angezeigt wird. Über das Thunderbird-Hauptmenü **[Extras/Einstellungen/Erweitert/Reiter „Zertifikate“/Zertifikate/„Ihre Zertifikate“]** klicken Sie auf Ihr E-Mail-Zertifikat, um den Aussteller Ihres Zertifikates zu ermitteln. Bei Bedarf müssen fehlende Ausstellerzertifikate in Thunderbird importieren werden.

- S/MIME-Sicherheit einrichten

Über das Thunderbird-Hauptmenü **[Extras/Konten-Einstellungen/S/MIME-Sicherheit]** können Sie nun das jeweilige E-Mail-Zertifikat auswählen. Achten Sie hierbei auf die angezeigte Verwendung. Eventuell müssen Sie für die Verschlüsselung ein anderes Zertifikat auswählen.

Weitere Informationen zu aktuellen Versionen der E-Mail Clients finden Sie auf der OpenLimit FAQ Seite unter

https://www.openlimit.com/FAQv2/

unter **[E-Mail Clients/Thunderbird]**.

9 SSL-Authentisierung

Mit den Modulen der OpenLimit SignCubes Software sind Sie in der Lage, sich an einer Webseite welche SSL-Authentisierung verwendet, anzumelden. Diese Aufgabe wird je nach Verwendung des Web-Browsers vom CSP oder vom PKCS#11 Treiber übernommen.

Über SSL

Secure Sockets Layer (SSL) ist ein Verschlüsselungsprotokoll für Datenübertragung im Internet. Wenn eine Verbindung zu einer Webseite über SSL hergestellt wird, geschieht dies in etwa so:

Zunächst sendet der Client (Web-Browser mit dem Sie arbeiten) eine Verbindungsanfrage an den Server (dort ist die Webseite, die Sie besuchen wollen). Daraufhin antwortet der Server und sendet ein Zertifikat. Indem Sie bestätigen, dass Sie dem Zertifikat des Servers vertrauen, ermöglichen Sie Ihren Web-Browser die Verbindung zum Server herzustellen. (Dieser Schritt wird unter Umständen automatisch durchgeführt, z.B. dann, wenn das Server-Zertifikat von Ihrem Web-Browser bereits als vertrauenswürdig eingestuft wird.) Eventuell will der Server aber auch wissen ob, Sie die Person sind, für die Sie sich ausgeben und sendet eine entsprechende Anfrage an Ihren Web-Browser (Bidirektionale SSL-Authentifizierung).Jetzt müssen Sie sich dem Server gegenüber identifizieren, indem Sie die Anfrage des Servers signieren. Dabei kommen die Module der Software zum Einsatz. Nun ist eine sichere Verbindung über SSL hergestellt.

Bitte beachten Sie, dass eine gegenseitige Identifizierung über SSL nicht das gleiche ist, wie eine SSL Verschlüsselung. Wenn Sie eine verschlüsselte Webseite besuchen, müssen Sie sich dem Server gegenüber nicht identifizieren. Zudem sendet der Server nicht unbedingt ein Zertifikat an Sie. Es wird zwar eine sichere Verbindung hergestellt, jedoch ist es möglich, dass Sie die Daten, die Sie übermitteln nicht an die Stelle senden, an die Sie diese zu senden glauben.

Wenn Sie mehr über SSL wissen wollen, lesen Sie unter

- http://de.wikipedia.org/wiki/Secure_Sockets_Layer

nach.

Die folgenden Web-Browser werden für die SSL-Authentisierung von OpenLimit CC Sign 2.8 unterstützt:

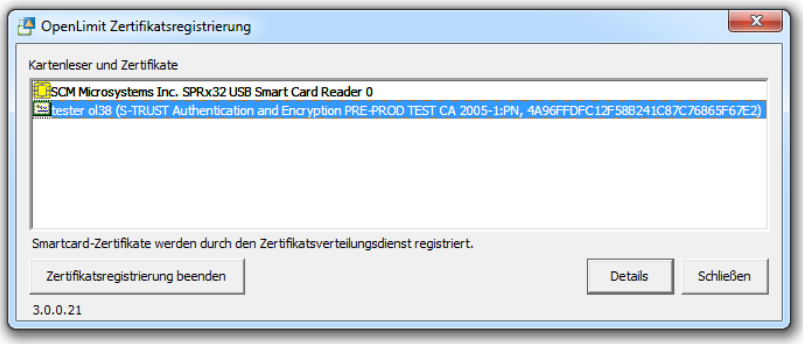
- Internet Explorer ab Version 6
- Firefox ab Version 3

Der Internet Explorer nutzt dazu den Cryptographic Service Provider (CSP). Firefox hingegen verwendet den PKCS#11 Treiber. Firefox muss im ersten Schritt konfiguriert werden, bevor die SSL-Authentisierung gestartet werden kann. Wenn Sie mit Firefox arbeiten, lesen Sie deshalb bitte die Kapitel Firefox Browser Sicherheitseinstellungen.

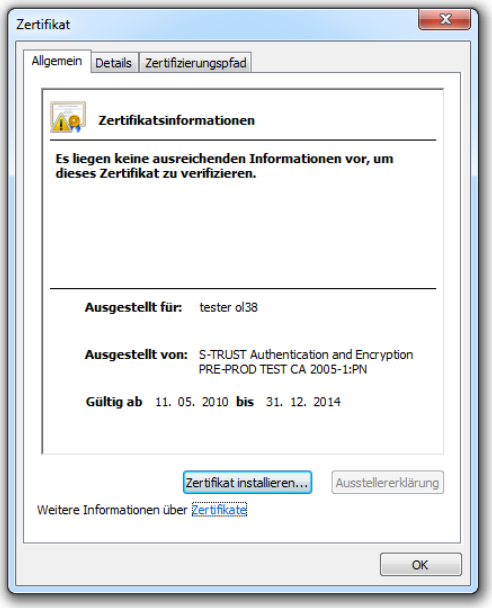
9.1 Internet Explorer

Bevor Sie eine Webseite besuchen können, welche mit SSL-Authentisierung arbeitet, müssen Sie Ihre Karte in den Kartenleser stecken und warten bis diese erkannt wurde (Chipsymbol ist gelb).

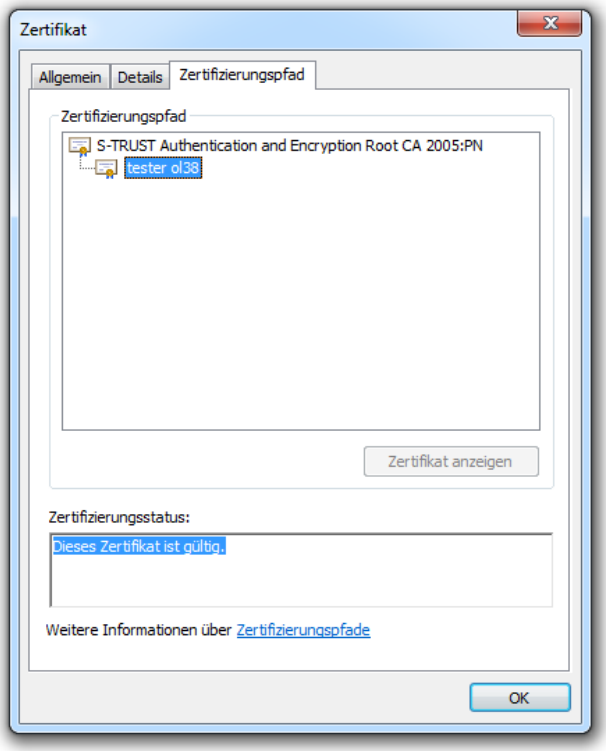
Prüfen Sie im nächsten Schritt, ob der Zertifizierungspfad Ihres Zertifikats im Zertifikatsspeicher des Microsoft Betriebssystems vollständig angezeigt wird. Klicken Sie dazu in der Taskleiste auf das Icon für die OpenLimit Zertifikatsregistrierung:



Wählen Sie das Zertifikat aus und bestätigen den Button **[Details]**.



Wählen Sie das Register **[Zertifizierungspfad]**:



Beim Start der Webseite wird eventuell eine Meldung angezeigt, in der Sie gefragt werden, ob Sie die sichere Webseite anzeigen wollen.

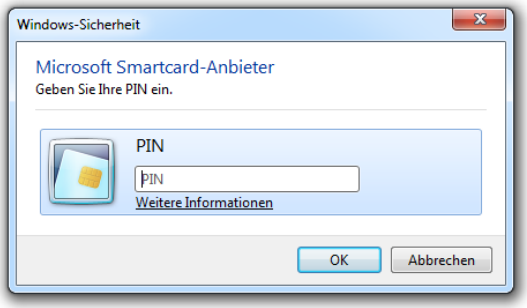
- Bestätigen Sie den Dialog mit **[Ja]**, um fortzufahren.

Jetzt werden Ihnen Sicherheitshinweise zum Zertifikat der angesteuerten Webseite angezeigt. Lesen Sie diese aufmerksam durch und lassen Sie sich das Zertifikat anzeigen.

- Um den Vorgang fortzusetzen, müssen Sie die Webseite als vertrauenswürdig akzeptieren.

In dem darauffolgenden Fenster wird Ihnen Ihr Zertifikat für die Anmeldung angezeigt, bestätigen Sie dies mit **[OK]**:

Anschließend werden Sie zur Eingabe der PIN für das fortgeschrittene Zertifikat (globale PIN bzw. CSP Passwort) aufgefordert. Geben Sie diese PIN über die Tastatur ein.



Die Verbindung zur Webseite wird hergestellt. Alle Daten, die nun zwischen Ihnen und der Webseite ausgetauscht werden, werden über eine sichere Verbindung geschickt.

9.2 Firefox Browser

Bevor Sie die SSL-Authentisierung verwenden können, müssen Sie den Web-Browser so konfigurieren, dass dieser mit Ihrer Smartcard und den darauf installierten Zertifikaten umgehen kann.

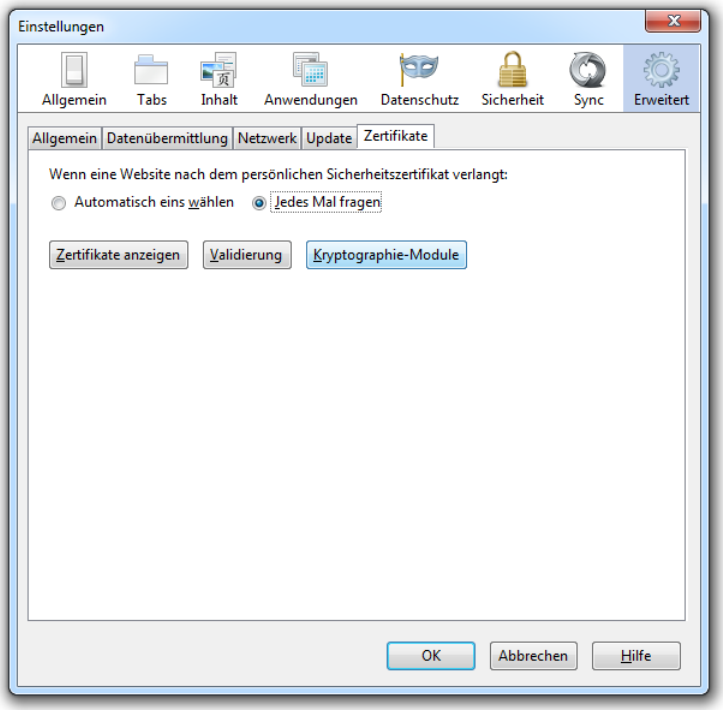
9.2.1 Firefox Browser Sicherheitseinstellungen

Die Beschreibungen in diesem Kapitel setzten voraus, dass Ihr Kartenleser richtig installiert ist, Ihre Karte sich in diesem befindet, erkannt wurde und die notwendigen Zertifikate sich auf Ihrer Karte befinden.

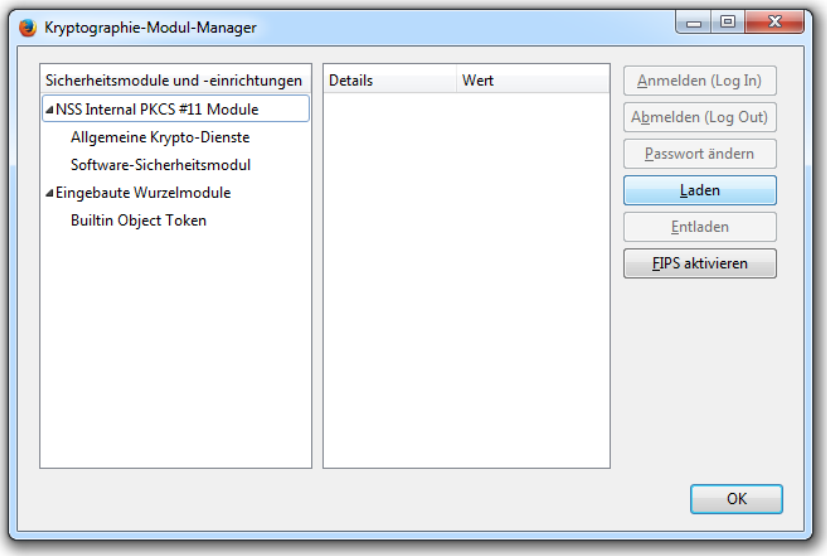
- Öffnen Sie den Web-Browser und klicken Sie dann in der Menüleiste auf **[Extras/Einstellungen]**.

Kryptographie Modul installieren

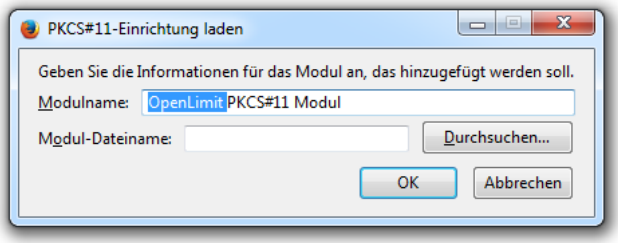
- Wählen Sie nun aus der Spalte links im Fenster **[Erweitert]** und das Register **[Zertifikate]** und klicken auf den Button **[Kryptographie-Module]**:



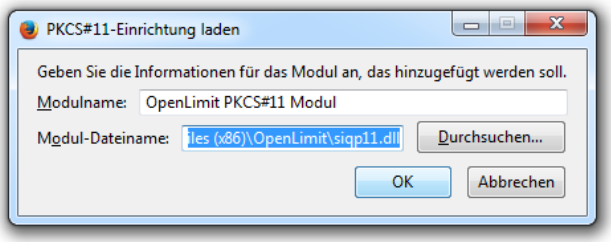
- Bestätigen Sie den Button **[OK]** und bestätigen den Button **[Laden]**:



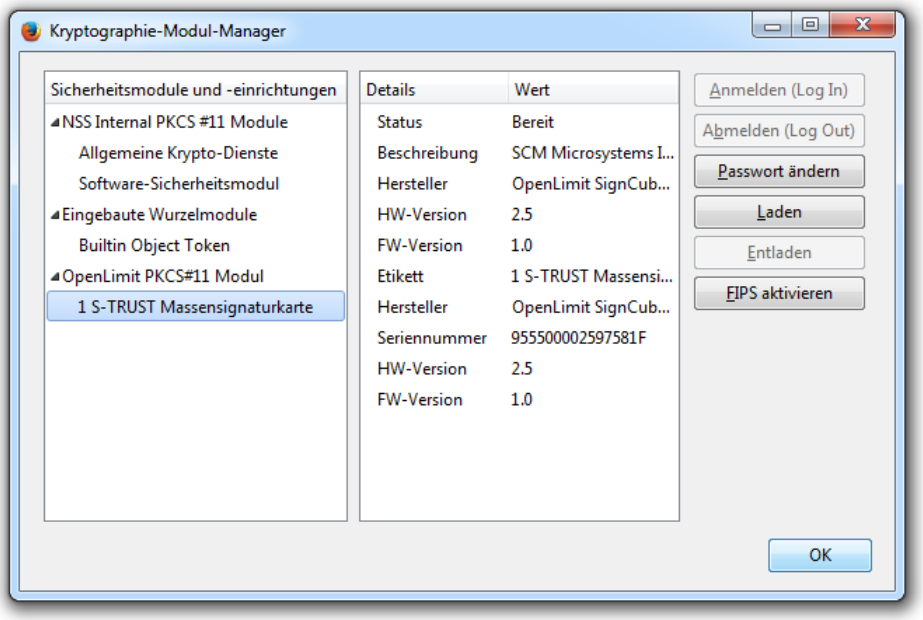
In dem darauffolgenden Fenster tragen Sie unter Modulname einen Namen ein, z.B. OpenLimit PKCS#11 Modul:



Wählen Sie über **[Durchsuchen]** die Datei „siqp11.dll im OpenLimit Programmeordner (standardmäßig in **C:\Program Files (x86)\OpenLimit**) und bestätigen die Auswahl mit **[OK]**:



Es öffnet sich der Kryptographie-Modul-Manager mit der Ansicht der aktiven Komponenten einschließlich der OpenLimit-Komponente:



- Klicken Sie nun auf **[OK]**.

Jetzt ist Firefox für die SSL-Authentisierung konfiguriert.

9.2.2 Firefox SSL-Authentisierung

Bevor Sie eine Webseite besuchen können, welche mit SSL-Authentisierung arbeitet, müssen Sie Ihre Karte in den Leser stecken und warten, bis diese erkannt wurde (gelbes Chipsymbol).

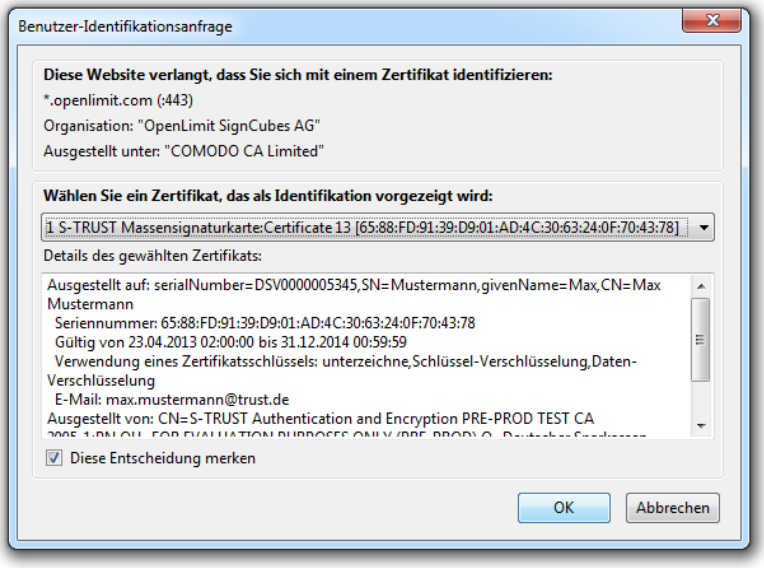
Herstellen einer Verbindung zu einer Webseite mit SSL-Authentisierung

Wenn Sie mit Firefox eine Webseite aufsuchen, die SSL-Authentisierung verwendet, wird eventuell eine Meldung angezeigt, in der Sie gefragt werden, ob Sie die sichere Webseite anzeigen wollen.

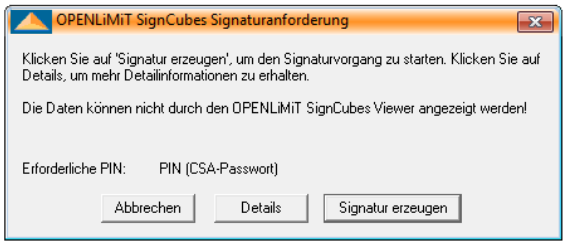
Jetzt werden Ihnen Sicherheitshinweise zum Zertifikat der angesteuerten Webseite angezeigt. Lesen Sie diese aufmerksam durch und lassen Sie sich das Zertifikat anzeigen. Um den Vorgang fortzusetzen, müssen Sie diesem Zertifikat vertrauen und mit **[Ja]** bestätigen.

Sie können das Zertifikat temporär oder für immer akzeptieren. Wenn Sie das Zertifikat für immer akzeptieren, wird es im Zertifikats-Manager abgelegt und beim nächsten Besuch der Webseite nicht mehr

angezeigt. Anschließend wird das Zertifikatsauswahlfenster geöffnet. Bestätigen Sie das Zertifikat mit **[OK]**.



Es wird der Signaturanforderungsdialog der OpenLimit Software gestartet.



- Klicken Sie jetzt auf den Button **[Signatur erzeugen]**.
- Geben Sie Ihre globale PIN (CSA-Passwort) ein. Damit identifizieren Sie sich gegenüber dem Server.

Es wird die Verbindung zur Webseite hergestellt. Alle Daten, die nun zwischen Ihnen und der Webseite ausgetauscht werden, werden über eine sichere Verbindung geschickt.

10 Technischer Support

Bei Fragen in der Arbeit mit dem Produkt OpenLimit CC Sign 2.8 sollten Sie zunächst die Beschreibung in dem entsprechenden Kapitel des elektronischen Handbuches bzw. in der „Online Help“ der OpenLimit SignCubes Basiskomponenten 2.8, Version 2.8.0.1 nachlesen.

Fehlermeldungen und Erklärungen finden Sie in der „Online Help“ im Kapitel „Erste Hilfe“.

Darüber hinaus steht Ihnen zur Unterstützung ein telefonischer Support zur Verfügung. Weitere Informationen zum technischen Support und zu häufig gestellten Fragen (FAQ) finden Sie im Internet unter:

- https://www.openlimit.com/de/support/service.html

Vorab sollten Sie sich darüber informieren, welche Softwareversion Sie installiert haben. Diese Meldung finden Sie unter **[Start/Alle Programme/OpenLimit/Versionsinformation]** bzw. **[Apps/OpenLimit/Versionsinformation]**.