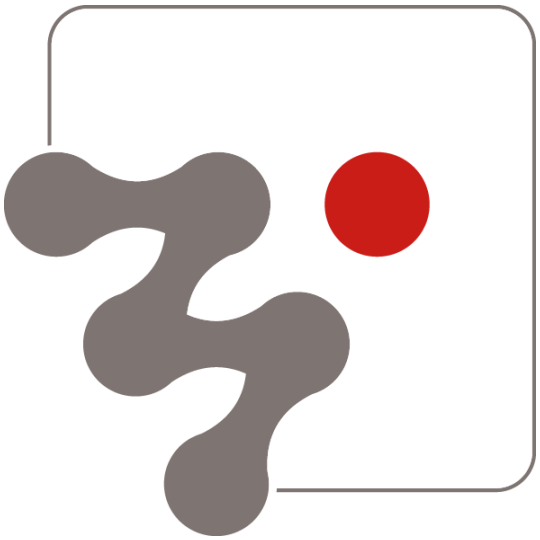


AutoVerifier DataCenter-Edition

V 2.1.25

(Windows)

Anwenderhandbuch

Version 2.3

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

Tel: +49 5063 / 2 77 4 -0
Fax: +49 5063 / 2 77 44 -50
Service Center: 01805 - 691 188 (Bundesweit 12 Cent/min)

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

1 Inhalt

1 Inhalt 3
1.1 Änderungshistorie 5
1.2 verwendete Textformate 5
2 Einleitung 6
2.1 Funktionsweise 6
2.1.1 Prinzipielle Arbeitsweise 6
2.1.2 Probleme bei Dateizugriffen 6
2.2 Systemvoraussetzungen 7
3 Installation 8
3.1 Lizenz-Datei 9
4 Verwenden 11
4.1 Der AV DCE Dienst 11
4.1.1 Dienste-Steuerung 11
4.1.2 AVService.exe 12
4.2 Die GUI 14
4.2.1 Datei 15
4.2.2 Einstellungen 15
4.2.3 Verifikation 28
4.2.4 OCSP-Responder 33
4.2.5 Verzeichnisüberwachung 36
4.2.6 SOAP-Connector (Zusatzmodul) 42
4.2.7 Remote-Konsole 43
4.2.8 Werkzeuge 47
4.2.9 Hilfe 48
4.3 DCE-Webkonsole 49
4.4 Konfigurationsdatei 49
4.4.1 Server 49
4.4.2 AV DCE GUI 50
5 Konfiguration 51
5.1 Konfig mit der AV DCE-GUI 51

5.2 Einstellungen direkt in der Konfigurationsdatei 52
5.2.1 GUI-Einstellungen 52
5.2.2 Anwendungsmodi 52
5.2.3 Sprache 53
5.2.4 Prozessanzahl 53
5.2.5 Logging 53
5.2.6 Remoteconnector 55
5.2.7 Session 55
5.2.8 SSL-Verifikation 55
5.2.9 Verifikationsmodus 59
5.2.10 Die Dateisystem-Schnittstelle 60
5.2.11 Soap Engine 61
5.2.12 SMTP-Engine 61
6 Log-Ausgaben 62
7 Anhang 64
7.1 PlugIns 64
7.1.1 SOAP-Connector/ SMTP-Connector 64
7.2 Fehlercodes 64
7.3 SQL-Datenbank Protokollierung 70
7.3.1 Script zur Erstellung der Tabellen und Schlüssel (SQL-Logging) 70
7.3.2 Script zur Erstellung der Sicht „showevents“ 73
7.3.3 Einrichtung Zugang 73
7.4 Beispiel Config.xml 76
7.5 AVPDF-Service 80
7.6 SOAP-Connector 80
7.7 weiterführende Infos 82
7.8 Abbildungsverzeichnis 83
7.9 Stichwortverzeichnis 85

Stand: 24.10.2016 09:19

1.1 Änderungshistorie

Version	Datum	Änderung	Verfasser
1.1	01.07.2010	Erstellung der ersten Fassung	Stefanie Böhme
2.1	17.01.2011	Anpassung	Stefanie Böhme
2.2	24.05.2013	Anpassung	Olaf Meinecke
2.3	24.10.2016	Überarbeitet	Bernd Hohmann

1.2 verwendete Textformate

Normaler Text ist nicht speziell gekennzeichnet. *Bildunterschriften* sind in kleinerer Schrift dargestellt. GUI-Elemente werden speziell markiert. `SourceCode` und `Dateinamen` werden ebenfalls in anderer Schriftart kenntlich gemacht.

2 EINLEITUNG

Das vorliegende Handbuch macht Sie mit der Verifikationsanwendung **Autoverifier Data Center Edition** (AV DCE) für Windows[1] bekannt. Es wendet sich an Anwender und Administratoren, welche die Verifikationsanwendungskomponente AV DCE installieren und verwenden wollen. Dieses Handbuch beschreibt die

- Installation
- Enrichtung
- Verwendung

der gelieferten Software.

2.1 Funktionsweise

2.1.1 Prinzipielle Arbeitsweise

Der AutoVerifier Data Center Edition läuft als Dienst und prüft regelmäßig, ob sich Dateien in einem zu überwachenden Verzeichnis[2] befinden. Diese Dateien werden dann automatisch verarbeitet. Verarbeitete Daten und ggf. weitere Verarbeitungsergebnisse werden in entsprechenden Ausgangsordnern abgelegt.

2.1.2 Probleme bei Dateizugriffen

Im laufenden Betrieb kann es zu Fehlern bei der Dateibearbeitung kommen. Während der AV DCE auf Dateien im Eingangsverzeichnis zugreifen will, die gerade dort erstellt werden, oder wenn der AV DCE Dateien im Ausgangsverzeichnis erzeugen will, bzw. erzeugt und diese eventuell in eine Weiterverarbeitung eingebunden sind, kann es zu Zugriffsverletzungen kommen.

Um diese Fehler zu vermeiden, verwendet der AV DCE einen Schutzmechanismus:

- solange sich im Eingangsverzeichnis eine Datei *.upload* befindet, wird keine Abarbeitung einer Datei durchgeführt
- solange im Ausgangsverzeichnis eine Datei *.download* gefunden wird, wird der Verifikationsvorgang ebenfalls nicht gestartet

[1] Für die Linux-Version gibt es ein Extrahandbuch.
[2] Sofern kein anderer Modus konfiguriert wurde.

Diese Dateien signalisieren, dass in den entsprechenden Verzeichnissen im Augenblick Dateioperationen stattfinden. Der AutoVerifier Data Center Edition versucht dann periodisch, erneut einen Verifikationsdurchlauf zu starten. Dieses wiederholt sich bis die *.upload* und/oder die *.download* Datei gelöscht wurde.

Wird vom AutoVerifier Data Center Edition ein Verifikationsdurchlauf gestartet, wird im Eingangs- und Ausgangsverzeichnis je eine Datei mit Namen *.running* erstellt. Nach Beendigung des Verifikationslaufs werden diese Dateien automatisch wieder gelöscht.

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

2.2 Systemvoraussetzungen

Für die Installation der Software gelten folgende Systemvoraussetzungen:

- Installierte Stammzertifikate deutscher und internationaler Trustcenter (werden teilweise mit ausgeliefert)
- Eine gültige Lizenzdatei
- Betriebssystem aus folgender Liste:
  - Windows 2008 Server
  - Windows 2012 Server
  - Windows Vista SP1
  - Windows 7
  - Windows 8

Die Systemvoraussetzungen für die zusätzlichen Konnektoren entnehmen Sie bitte den entsprechenden Handbüchern.

3 INSTALLATION

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

Nach der Auswahl des Installationsortes wird der AutoVerifier Data Center Edition installiert.

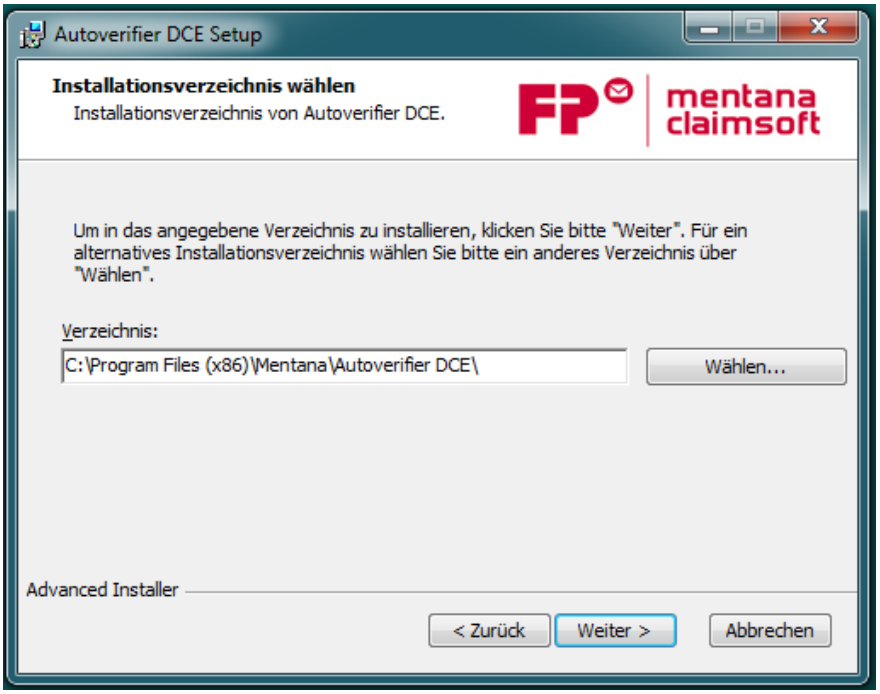


Abbildung 3-1 Auswahl des Installationsortes

Nach der Installation steht der entsprechende Systemdienst zur Verfügung, der unter dem Namen **Mentana AutoVerifier DCE** in der Windows-Dienstverwaltung (services.msc) gesteuert werden kann.

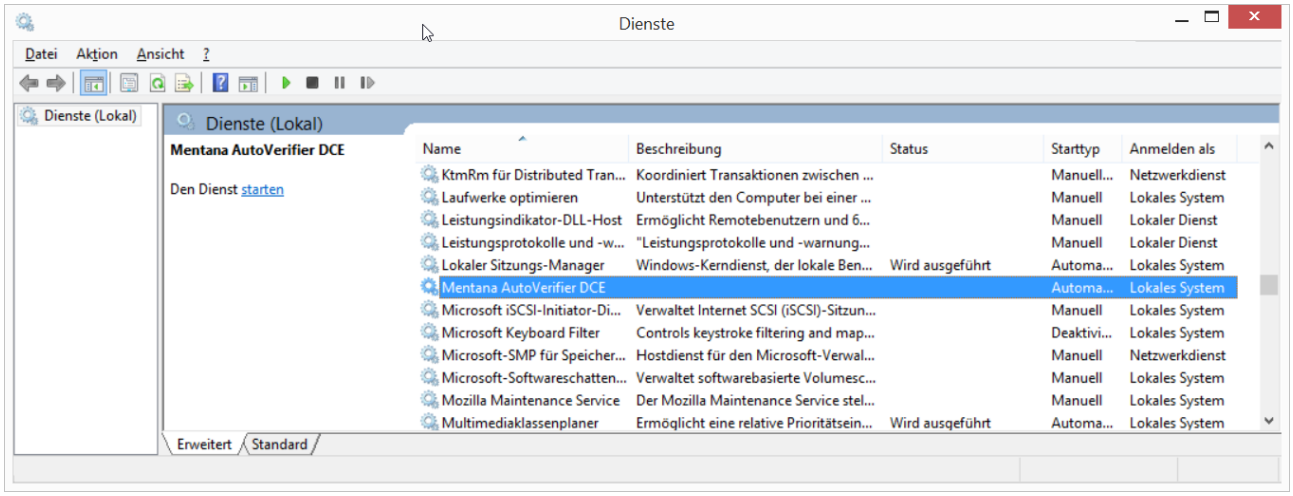


Abbildung 3-2 AutoVerifier DCE in der Windows-Dienstverwaltung

3.1 Lizenz-Datei

Für die korrekte Funktion des AV DCE wird eine Lizenz-Datei benötigt. Diese wird gesondert von Mentana-Claimsoft GmbH für den Kunden angefertigt und versandt. Die Datei `license.xml` muss in das Verzeichnis des AV DCE kopiert werden.
(z.B.: `C:\Program Files (x86)\Mentana\Autoverifier DCE`)

Beim Starten des AV DCE-Dienstes wird die Lizenz überprüft und nur bei gültiger Lizenz ist das Programm lauffähig.

Die GUI überprüft ebenfalls die Lizenzdatei. Beim Start wird das Ergebnis im Log angezeigt.

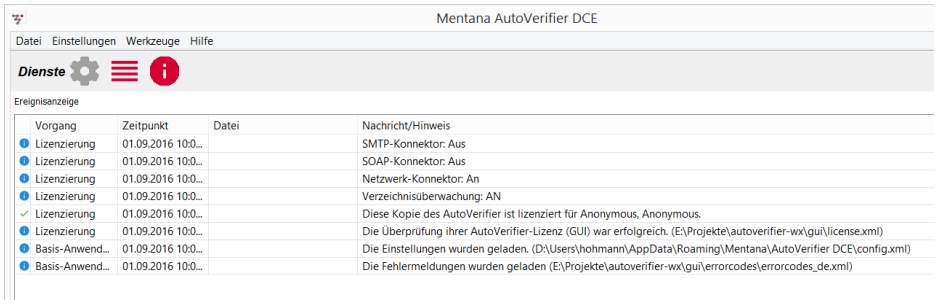


Abbildung 3-3 Lizenzprüfung

Später im laufenden Betrieb kann man die korrekte Lizenz unter
Einstellungen / Allgemeine Einstellungen kontrollieren:

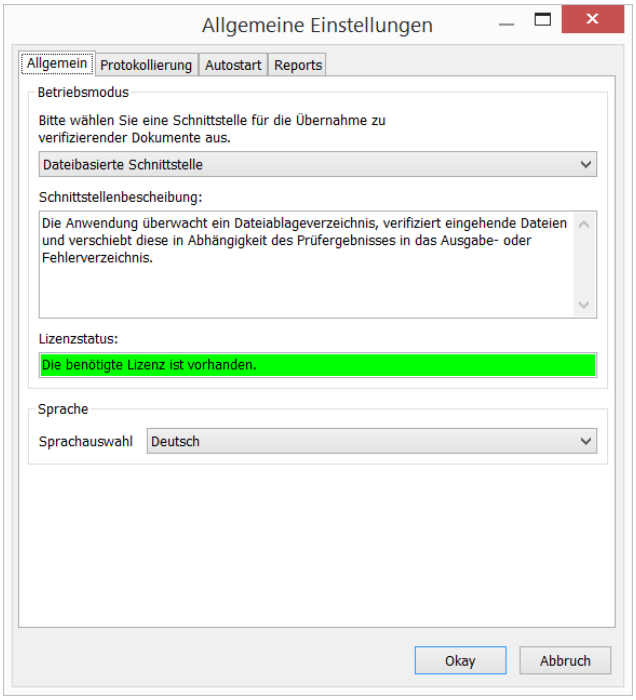


Abbildung 3-4 Allgemeine Lizenzanzeige

Startet man die AV DCE GUI, so wird ebenfalls die Lizenz-Datei zur Überprüfung geöffnet. Hierfür muss die mitgelieferte Lizenz-Datei des Services in das Verzeichnis der Konfig-GUI kopiert werden. Die GUI sucht nur im aktuellen Verzeichnis nach einer Lizenz.

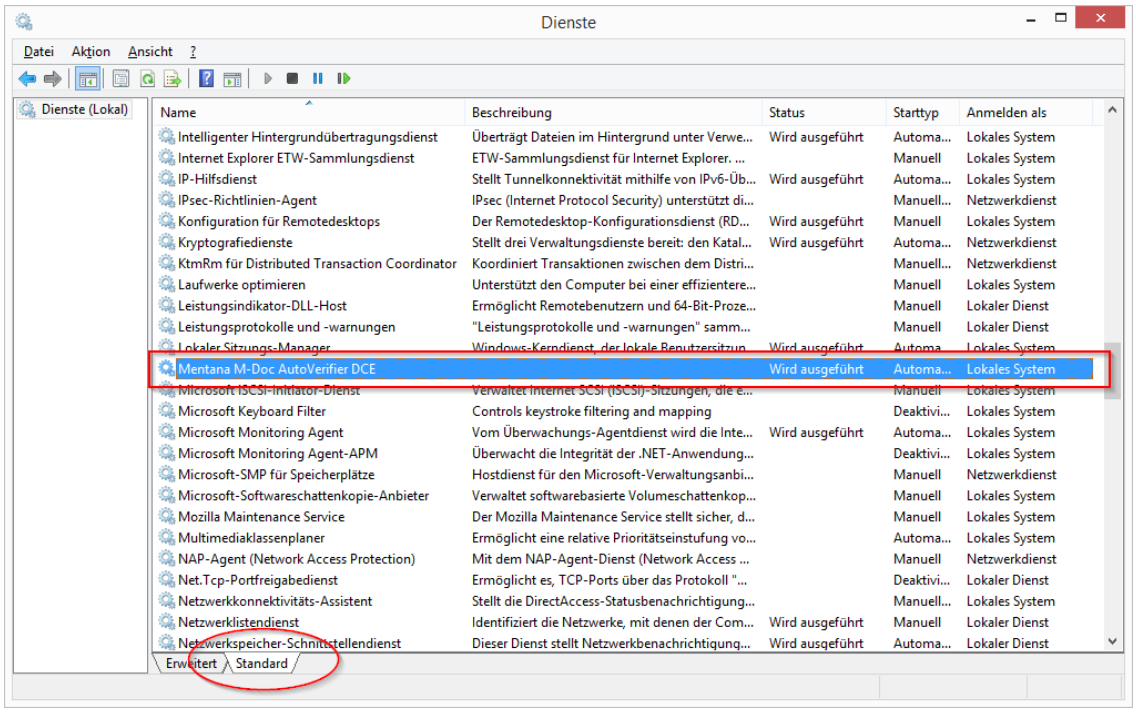
4 VERWENDEN

4.1 Der AV DCE Dienst

Der Autoverifier DCE läuft als Dienst: dieser installierte Dienst verarbeitet die Verifikationsanforderungen. Über die AV DCE GUI wird die Konfiguration (Dienstunabhängig) durchgeführt.

4.1.1 Dienste-Steuerung

Öffnet man die Windows-Dienstverwaltung (services.msc), so findet man dort den Mentana AutoVerifier DCE-Dienst.



AutoVerifier DCE in der Windows-Dienstverwaltung

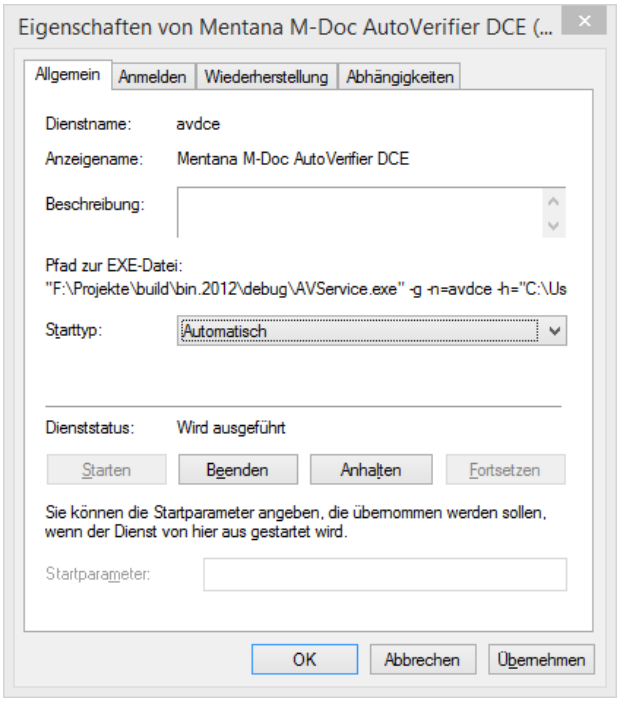


Abbildung 4-1 Eigenschaften des AV DCE-Dienstes

4.1.2 AVService.exe

Die Steuerung des Dienstes kann aus der Dienste-Steuerung geschehen. Alternativ können Sie den AutoVerifier Data Center Edition als Konsolen-Anwendung verwenden. Für das Starten aus der Konsole heraus, benötigt diese allerdings den den Administrator-Modus.

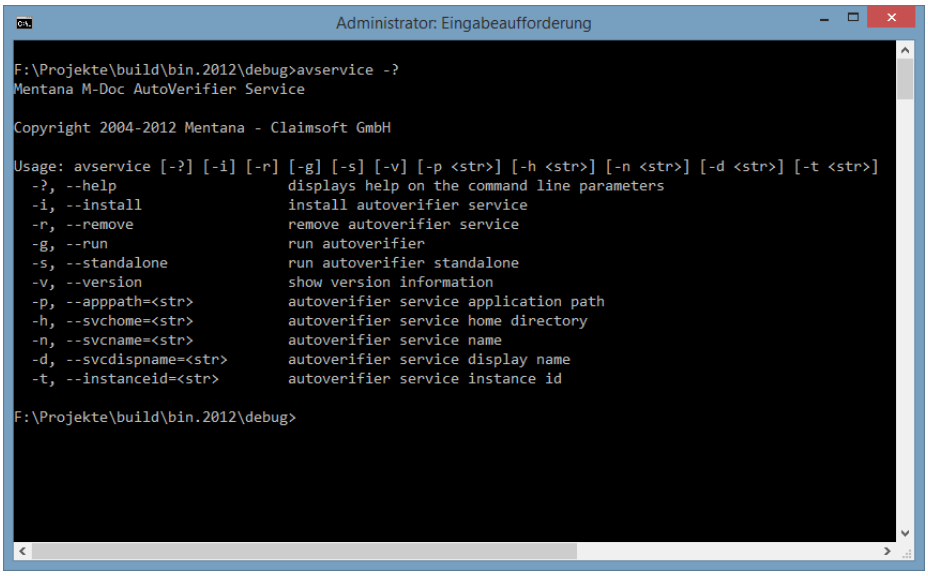


Abbildung 4-2 Konsole im Admin-Modus

Die AVService.exe hat folgende Aufrufparameter:

Parameter	*Parameter*	*Erklärung*
-?	help	Zeigt die Hilfe in der Kommandozeile an.
-i	install	Installiert den AutoVerifier Service.
-r	remove	Deinstalliert den AutoVerifier Service.
-g	run	Startet den AutoVerifier Service.
-v	version	Zeigt die Versions Informationen.
-p	apppath=<str>	Gibt den Pfad der Anwendung an.
-h	svchome=<str>	Gibt den Pfad des Homeverzeichnisses an
-n	svcname=<str>	Gibt den Dienstnamen an (muss eindeutig sein).
-d	svcdispname=<str>	Gibt die Serviceanzeigenamen an (muss eindeutig sein).
-t	instanceid=<str>	Setzt eine optionale Instanz ID. (optional)
-l	<keiner>	schaltet internes Logging an

Beispiele:

```
avservice -i -n avdce_svcname -d avdce_svcbeschreibung -t avdce_instanz
```

Installiert den AV DCE als Dienst mit Namen „avdce_svcname“:

Die Config-Datei der Dienstedatei wird aus
`C:\ProgramData\Mentana\AutoVerifier DCE\`
ausgelesen. In diesem Verzeichnis sucht der Dienst auch nach der gültigen Lizenzdatei.

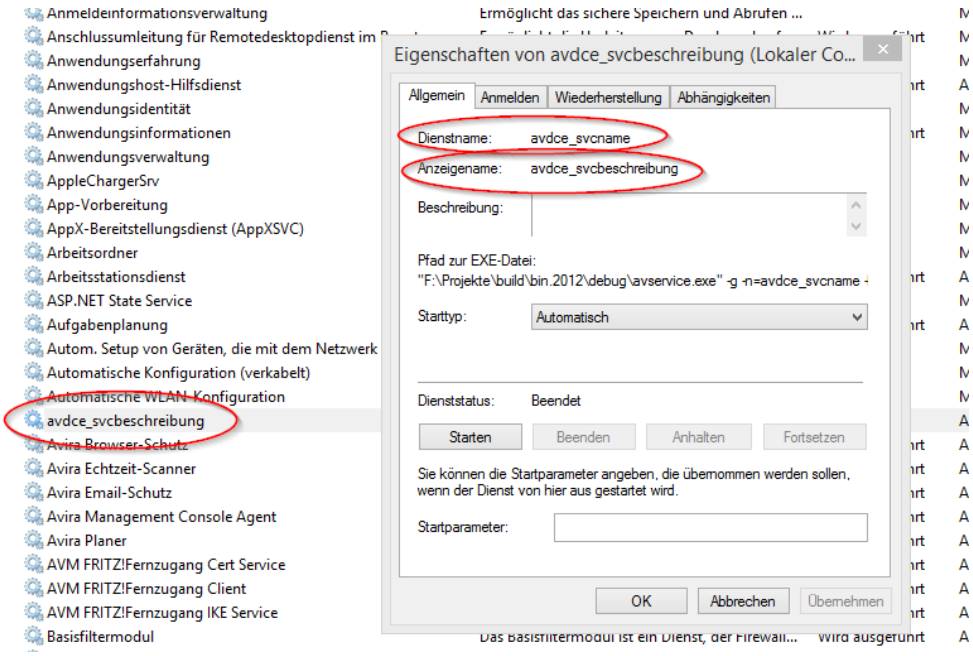


Abbildung 4-3 Der installierte AVDCE im Dienstmanager

4.2 Die GUI

Wird die AV DCE-GUI gestartet, wird ein Fenster ähnlich diesem gestartet:

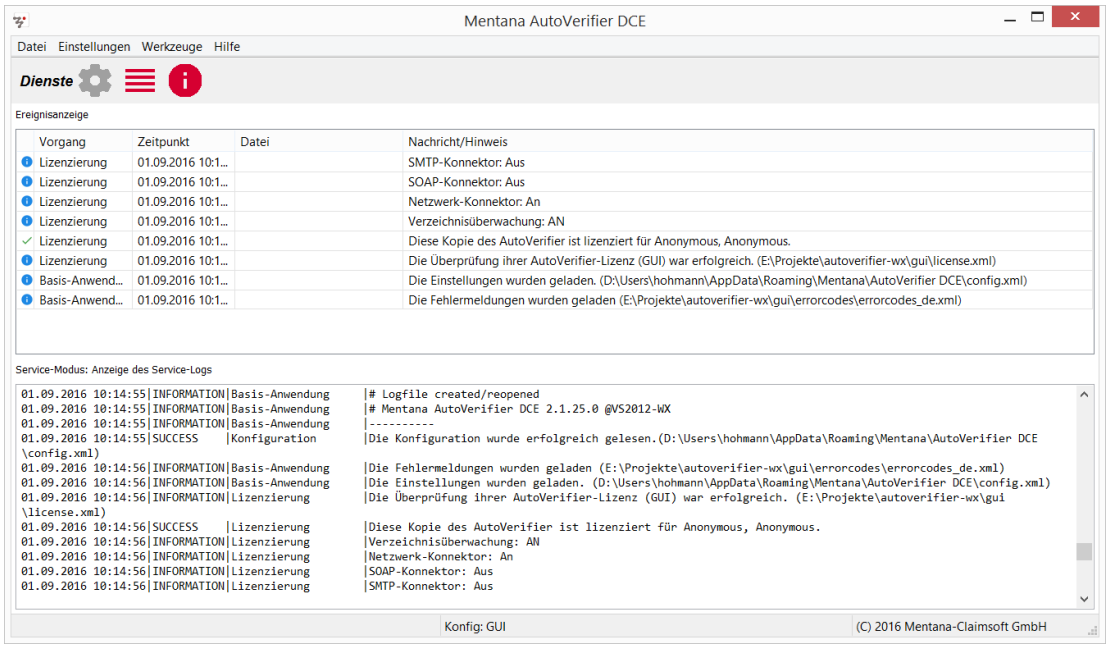


Abbildung 4-4 GUI im Dienst-Modus mit Service-Logging

Im oberen Bereich befindet sich eine Symbolleiste:

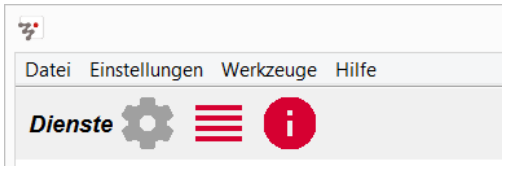


Abbildung 4-5 Symbolleiste Dienst-Modus (zuwenig Rechte)

Anm.: Eine Steuerung des Dienstes (Start/Stop) kann nur erfolgen, wenn die GUI als Administrator gestartet wurde.

Die Bedeutung der Schaltflächen ist hier:

	Steuerung des Dienstes (Deaktiviert wg. Admin-Rechten)
	Dienstesteuerung aktiviert
	Logfile des Dienstes anzeigen (automatische Anzeige erfolgt alle 10sec)
	Programm-Infos anzeigen

4.2.1 Datei

4.2.1.1 Beenden

Die AV DCE GUI kann hierüber beendet werden.

4.2.2 Einstellungen

4.2.2.1 Allgemeine Einstellungen

Die allgemeinen Einstellungen sind auf vier Seiten aufgeteilt:

- Allgemein
- Protokollierung

- Autostart
- Reports

4.2.2.2 Allgemein

Auf der Seite der allgemeinen Einstellungen können folgende Parameter eingestellt werden:

- Betriebsmodus des AV DCE
- die Sprache

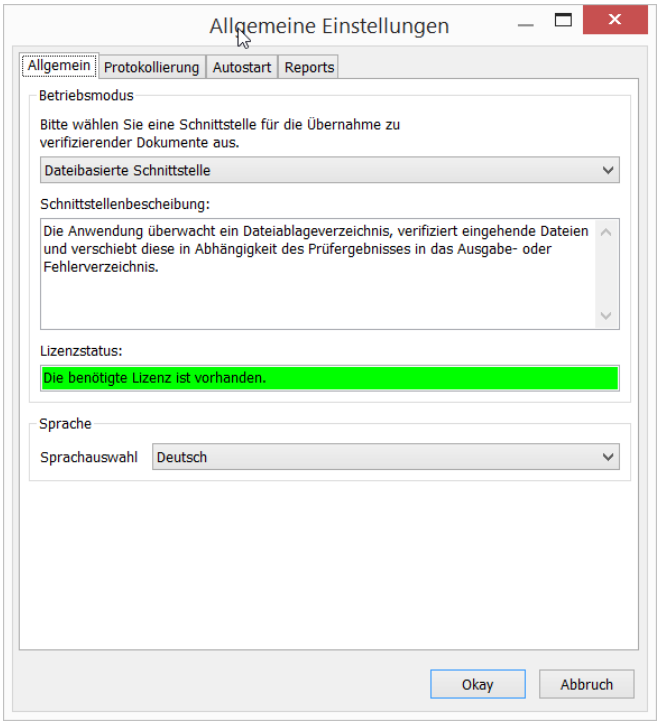


Abbildung 4-6 Allgemeine Einstellungen

Durch das Betätigen des OK Buttons werden Änderungen übernommen und in die Datei `config.xml` abgespeichert.

Nach Betätigen des Buttons Abbrechen werden die vorgenommenen Änderungen wieder verworfen bzw. die aktuellen Einstellungen beibehalten.

Betriebsmodus

Mögliche Schnittstellen für den Betriebsmodus sind:

Dateibasierte Schnittstelle

Die Anwendung überwacht ein Dateiablageverzeichnis, verifiziert eingehende Dateien und verschiebt diese in Abhängigkeit des Prüfergebnisses in das Ausgabe- oder Fehlerverzeichnis.

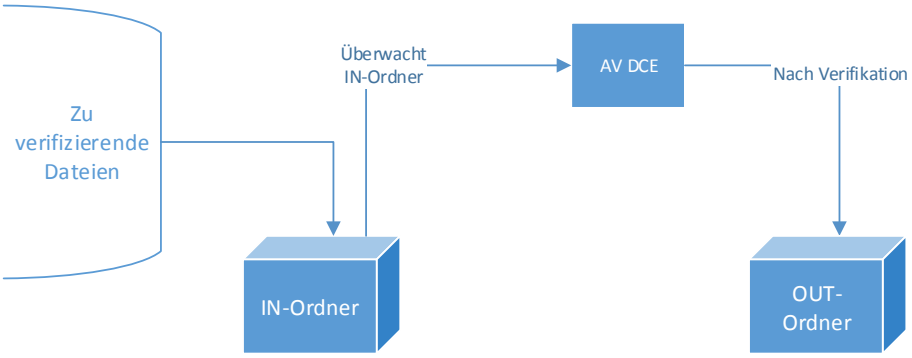


Abbildung 4-7 Schema Dateibasierte Schnittstelle

SOAP-Schnittstelle

Die Anwendung wird über eine Webservice-Schnittstelle (SOAP) gesteuert. Zu verifizierende Dokumente werden über einen SOAP-Endpoint übergeben und an den AutoVerifier weitergereicht

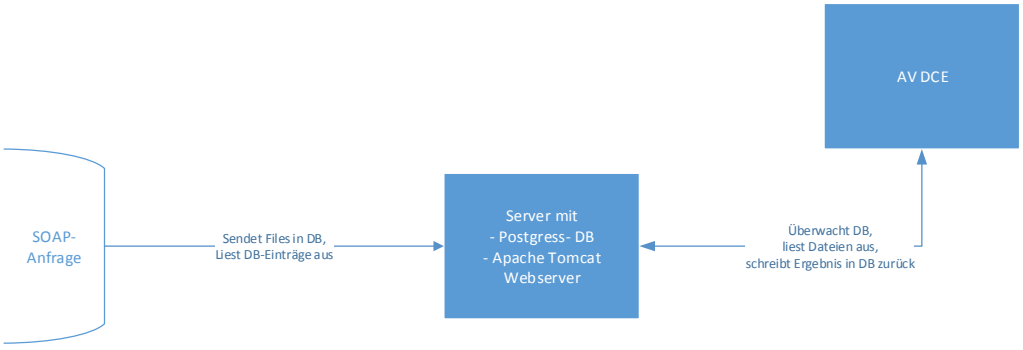


Abbildung 4-8 Schema SOAP-Schnittstelle

Für diese Funktionalität ist eine spezielle Lizenz erforderlich

SMTP-Schnittstelle

Die Anwendung arbeitet als transparenter E-Mail-Proxy innerhalb einer bestehenden E-Mail-Infrastruktur

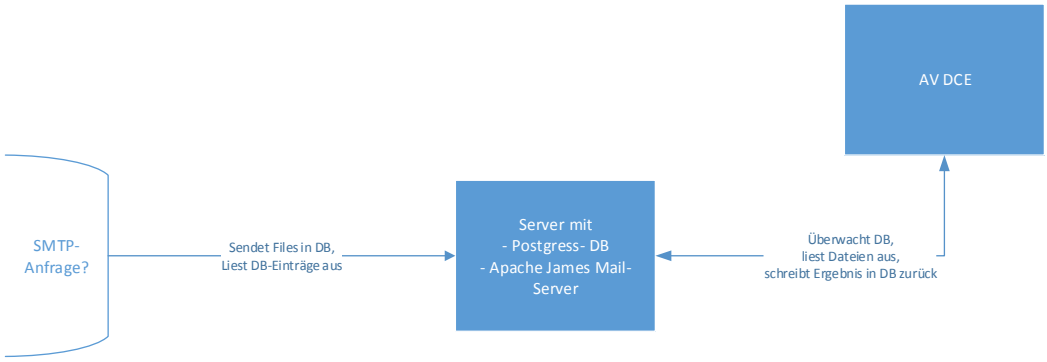


Abbildung 4-9 Schema SMTP-Schnittstelle

Für diese Funktionalität ist ebenfalls eine spezielle Lizenz erforderlich.

Verifikations-Einstellungen

Im Unterpunkt Verifikations-Einstellungen können Sie den Verifikationsmodus auswählen. Zur Auswahl stehen

- basierend auf dem Kettenmodell (SigG)
- basierend auf dem Schalenmodell

Für eine qualifizierte Verifikation von Signaturen ist der Modus „Kettenmodell (SigG)“ auszuwählen!

Sprache

Die Sprache des AV DCE kann derzeit zwischen Deutsch und Englisch gewählt werden.

4.2.2.3 Protokollierung

Unter Einstellungen / Allgemein kann auf der Seite Protokollierung die Einstellung vorgenommen werden, welche sich auf die Ereignisprotokollierung des AV DCE bezieht.

Die Einstellungen sind in folgende Bereiche unterteilt:

- interne Ereignisprotokollierung
- Ereignisprotokollieren

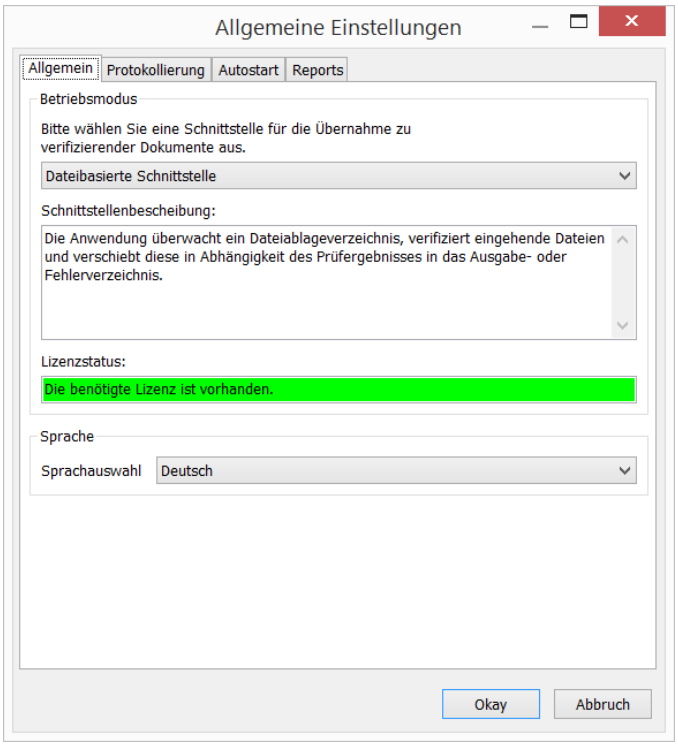


Abbildung 4-10 Protokollierung

Interne Ereignisprotokollierung

Der Schwellenwert der internen Ergebnisanzeige kann festgelegt werden. Vorausgewählt ist an diese Stelle der Grad „Alle Informationen“. Dies bedeutet, in der Ereignisanzeige werden sämtliche Ereignisse protokolliert.

Die Anzahl und Art der Meldungen lässt sich in der folgenden Abstufung variieren:

- *Alle Informationen* – Alle Ereignisse, die während des Verifikationsvorgangs auftreten.
- *Unkritische Informationen* – Ereignisse, die keinen Sicherheitsbezug haben.
- *Kritische Informationen* – Ereignisse, die einen Sicherheitsbezug haben.
- *Fehler* – Fehler, die eine Fortsetzung des Verifikationsvorgangs erlauben.

- *Ausnahmefehler* – Fehler, bei denen keine Fortsetzung des Verifikationsvorganges möglich ist.

Weiterhin kann man festlegen, ab welchem Meldungsgrad eine E-Mail-Benachrichtigung erfolgen soll:

- Alle Informationen
- Unkritische Informationen
- Kritische Informationen
- Fehler
- Ausnahmefehler

Für den E-Mail-Versand müssen entsprechende Einstellung erfolgen, welche über die Schaltfläche E-Mail Einstellungen aufgerufen werden können.

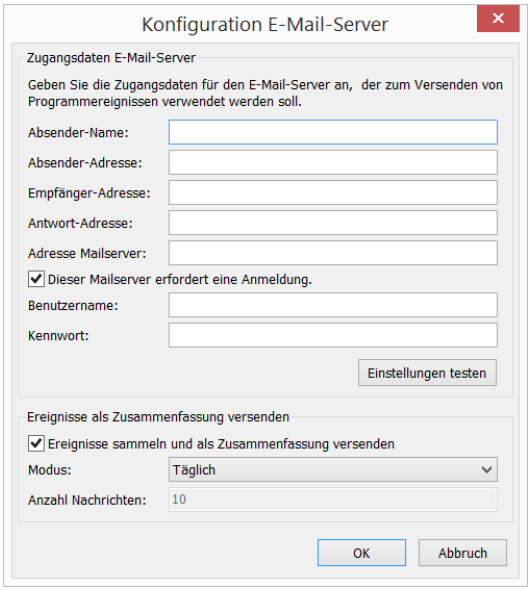


Abbildung 4-11 Konfiguration E-Mail-Server

Hier müssen folgende Angaben gemacht werden:

- *Absender-Name* – Hier muss der Absender-Name eingetragen werden.
- *Absender-Adresse* – Hier muss die Absender-Adresse eingetragen werden.
- *Empfänger-Adresse* – Hier muss die Empfänger-Adresse eingetragen werden.
- *Antwort-Adresse* – Hier muss die Antwort-Adresse eingetragen werden.

- *Adresse Mailserver* – Hier muss der SMTP-Server eingetragen werden.

Zusätzlich kann eingestellt werden, ob Nachrichten gesammelt werden sollen, so dass nicht jede Meldung als separate E-Mail versendet wird. Nachfolgende Möglichkeiten stehen für den Versand zur Verfügung:

- Stündlich
- Täglich
- Wöchentlich
- Erreichen einer bestimmten Nachrichtenzahl

Die korrekten E-Mail-Einstellungen können über die Schaltfläche [Einstellungen testen] auf Korrektheit geprüft werden.

Ereignisprotokollierung

Im Unteren Teil des Protokollierungsdialoges können Sie einen Protolldienst auswählen:

Es stehen zur Verfügung:

- *Textdatei-Protokollierung* – Log-Informationen werden im Textformat abgelegt.
- Datenbank-*Protokollierung* – Die zu protokollierenden Ergebnisse werden in einer SQL-Datenbank (vgl. Anhang 7.3) abgelegt

Je nachdem, welcher Dienst gewählt wurden, gelangt man über die Schaltfläche [Konfigurieren] zur entsprechden Eingabemaske für die Parameter des Dienstes:

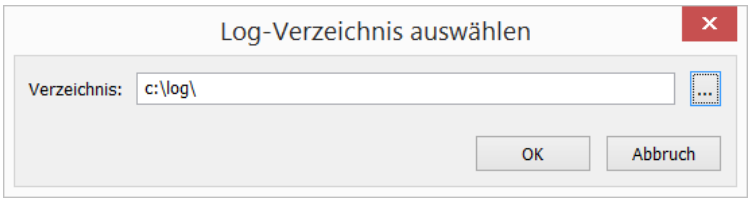


Abbildung 4-12 Log-Verzeichnis auswählen (Textdatei-Protokollierung)

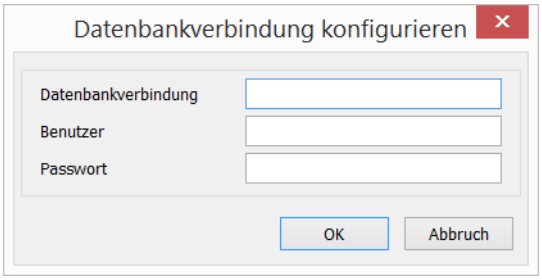


Abbildung 4-13 Parameter für die Datenbank-Protokollierung

Weitere Infos zur DB-Protokollierung siehe unter 7.3

4.2.2.4 Autostart

Nachdem Sie über Einstellungen/Allgemein zur Seite Autostart wechselt sind, können Sie durch aktivieren dieser Option die Verifikationssitzung nach Programmstart automatisch starten.

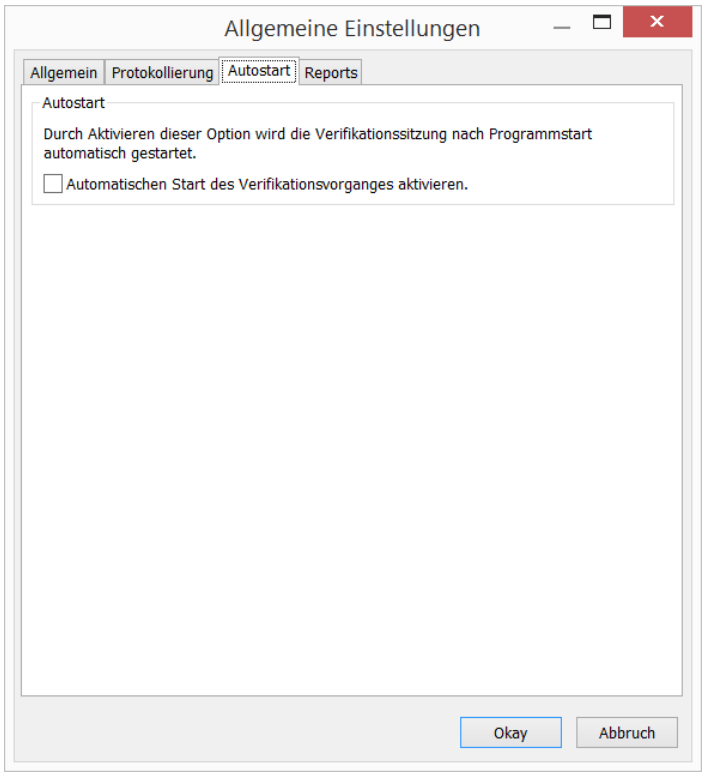


Abbildung 4-14 Allgemeine Einstellung – Autostart

4.2.2.5 Reports

Unter Einstellungen/Allgemein können Sie auf der Seite Reports verschiedene Einstellungen zu den Verfikationsberichten vornehmen. Die Einstellungen sind unterteilt in folgende Bereiche:

- *XML-Verifikationsbericht*
- *PDF-Verifikationsbericht*
- *PDF-Verifikationsbericht-Collection*
- *Zeitstempel*

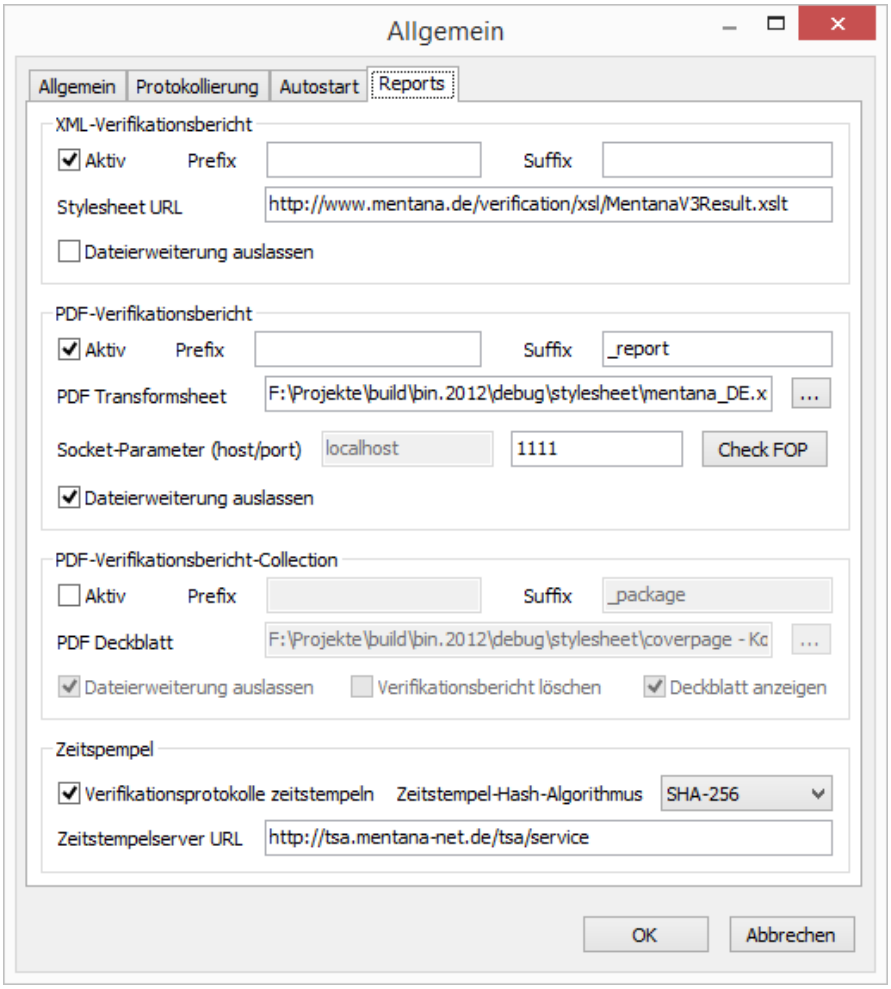


Abbildung 4-15 Report

XML-Verifikationsbericht

In diesem Bereich kann eingestellt werden, ob der AV DCE einen XML-Verifikationsbericht erstellen soll, wie dieser aussehen soll und wie die Benennung der Datei aussehen soll.

In der Checkbox Aktiv kann eingestellt werden, ob überhaupt eine XML-Datei erzeugt werden soll. (Es muss entweder XML-Bericht, PDF-Bericht oder beides aktiviert sein)

In den Textfeldern Prefix und Suffix können Texte eingetragen werden, welche den Dateinamen der verifizierten Datei erweitern, um so den Dateinamen der XML-Datei zu erzeugen:

Verifikation.pdf → <Prefix>Verifikation<Suffix>.pdf.xml

Bei der Dateinamenerzeugung der XML-Datei kann die Endung der Originaldatei ignoriert werden. Per Haken in der entsprechenden Checkbox wird dies angewählt.

Das Aussehen der XML-Datei wird über ein sog. Stylesheet gesteuert. Dies kann Online bei Mentana-Claimsoft GmbH heruntergeladen werden. Der aktuelle Ort für die Stylesheet-Url lautet:

http://www.mentana.de/verification/xsl/MentanaV3Result.xslt

Die XML-Datei mit dem Verifikationsbericht wird im Verzeichnis für die Ablage der Verifikationsreporte abgelegt (s.u.)

Anm.: Bei der Report-Erstellung wird immer zuerst eine XML-Datei erstellt. Aus dieser Datei wird dann das PDF/ die PDF-Collection o.ä. erzeugt. Ist die Erzeugung des XML-Verifikatsionsberichts nicht aktiviert, wird diese XML-Datei wieder entfernt, wenn sie für weiteren Gebraucht nicht mehr benötigt wird.

PDF-Verifikationsbericht

Die Möglichkeit der Erstellung eines PDF-Berichtes der Verifikation kann hier eingestellt werden. Der Dateiname der Berichtsdatei kann hier mit Prefix und Suffix aus der zu verifizierenden Datei erzeugt werden. Die Endung der Originaldatei kann dabei ausgelassen werden.

Für die zu erzeugende PDF-Datei wird ein Stylesheet verwendet. Dieses wird unter PDF Transformsheet benannt. Der Standardwert hierfür ist nach der Installation

stylesheet/mentana.xsl

Die Erzeugung der PDF-Datei erfolgt über einen Dienst, welcher den Apache Formatting Objects Processor (FOP) aufruft. Dieser Dienst wird beim Setup mit installiert und läuft standardmässig als AVPDFService.

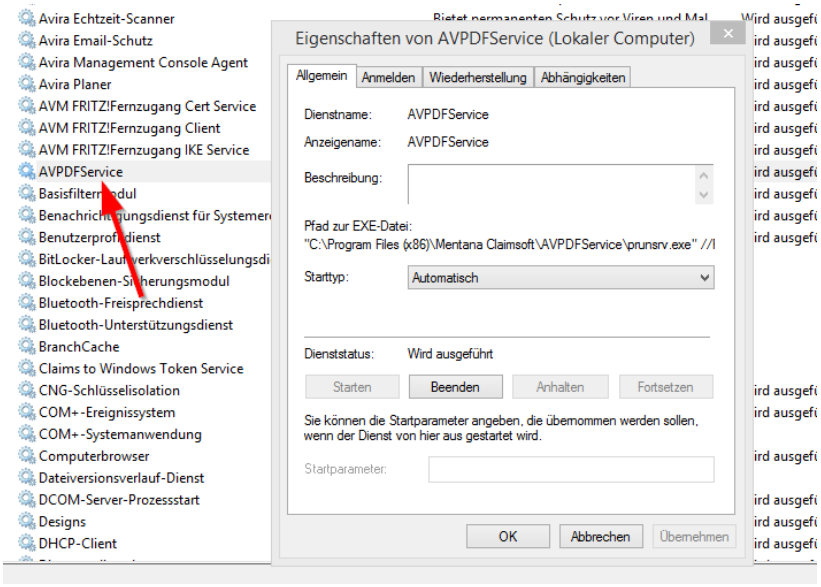


Abbildung 4-16 Liste der Dienste mit markiertem AVPDFService

Der Dienst „lauscht" auf Port 1111, um Aufträge für die PDF-Erstellung entgegen zu nehmen. Für weitere Infos zum AVPDFDienst siehe Kapitel 7.5.

In den allgemeinen Einstellungen muss aktuell nur der Port (hostname ist aktuell fest vorgegeben) eingestellt werden.

Ist dies erfolgt, kann über die Schaltfläche Check Fop der Status des Dienstes abgefragt werden. Bei installiertem, laufendem und erreichbarem Dienst erhält man folgende Meldung:

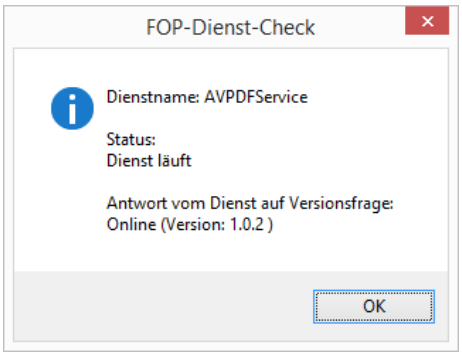


Abbildung 4-17 Erfolgreicher FOP-Check

Der Dienst meldet „Online", sowie seine aktuelle Versionsnummer als Info zurück. Diese wird angezeigt.

Wurde der Dienst beendet, bzw. nach der Installation noch nicht gestartet, so erhält man folgende Meldung:

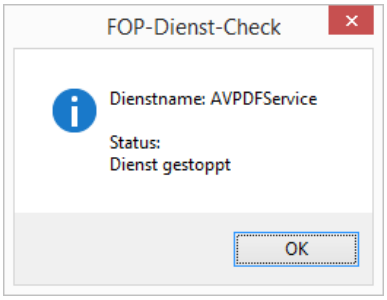


Abbildung 4-18 Gestoppter FOP-Dienst beim Check

Stimmt z.B. der Port zum Dienst nicht, erfolgt eine entsprechende Anzeige:

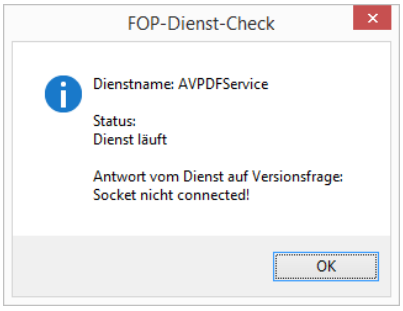


Abbildung 4-19 FOP-Dienst konnte via Socket nicht erreicht werden

Die Schaltfläche Check Fop ist allerdings nur aktiviert, wenn der AV DCE als Administrator gestartet wurde, da zum Auslesen der Dienste diese Rechte benötigt werden.

PDF-Verifikationsbericht-Collection

Der Verifikationsbericht kann zusammen mit der verifizierten Datei in einer PDF-Collection verpackt werden. Dies ist eine PDF-Datei, welche die genannten Datei als Anhänge beinhaltet. Mit einem PDF-Viewer hat man dann Zugriff auf die Inhalte.

Die Erzeugung der Collection kann per Haken in der Checkbox Aktiv an- bzw. ausgeschaltet werden. Der Dateiname der Collection-PDF-Datei kann hier ebenso wie zuvor mit Prefix und Suffix aus der zu verifizierenden Datei erzeugt werden. Die Endung der Originaldatei kann dabei ausgelassen werden.

Nach der Erzeugung der Collection besteht die Möglichkeit, den originalen Verifikationsbericht zu entfernen.

Eine PDF-Collection kann ein benutzerdefiniertes Deckblatt enthalten. Diese kann unter PDF-Deckblatt bestimmt werden und muss eine PDF-Datei sein.

Bei der Erstellung der Collection kann noch angegeben werden, ob das Deckblatt direkt angezeigt werden soll, wenn man die Collection im Viewer öffnet. Hierfür muss der Haken bei „Deckblatt anzeigen“ gesetzt werden.

Zeitstempel

Ein Verifikationsbericht vom AV DCE kann mit einem Zeitstempel versehen werden. Hierzu wird der Hashwert des Verifikationsprotokolles gebildet und an den Zeitstempel-Dienst gesendet. Das Ergebnis wird dann als tsr-Datei ebenfalls im report-Verzeichnis abgelegt. Es wird einfach der Name der Datei vom Verifikationsergebnis um diese Endung erweitert:

Verifikation.pdf → <Prefix>Verifikation<Suffix>.pdf.xml.tsr

Der zu benutzende Hash-Algorithmus für die Anfrage an den Zeitstempel-Dienst muss eingestellt werde. Möglich sind derzeit:

- SHA-256
- SHA-160

Weiterhin muss die URL für den Zeitstempelserver eingetragen werden. Bsp. ist dies:

http://tsa.mentana-net.de/tsa/service

4.2.2.5.1 Individuelle Anpassungen

Die die Coverpage, das XML-Stylsheet und das PDF-Stylesheet werden generell aus den in den Einstellungen eingetragenen Dateien benutzt. Sollte man jedoch für eine zu verifizierende Datei eigene Dateien benutzen wollen, muss man zusammen mit der zu überrüfenden Datei (z.B. test.pdf) die entsprechenden Dateien im IN-Verzeichnis ablegen:

- test.pdf.coverpage
- test.pdf.xmlstylesheet
- test.pdf.pdfstylesheet

Diese Dateien werden nach der Verarbeitung gelöscht.

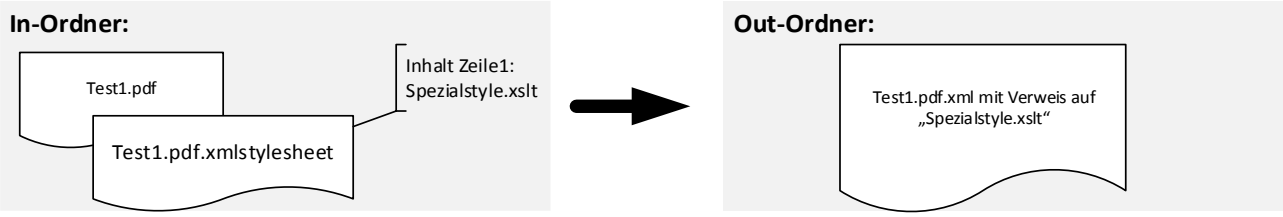
xmlstylesheet

Generell wird als Stylesheet für das XML-File, welches das Verifikationsergebnis enthält, die Vorgabe aus dem Setup benutzt. (Abbildung 5-2 AutoVerifier DCE ...Stylesheet URL). Möchte man

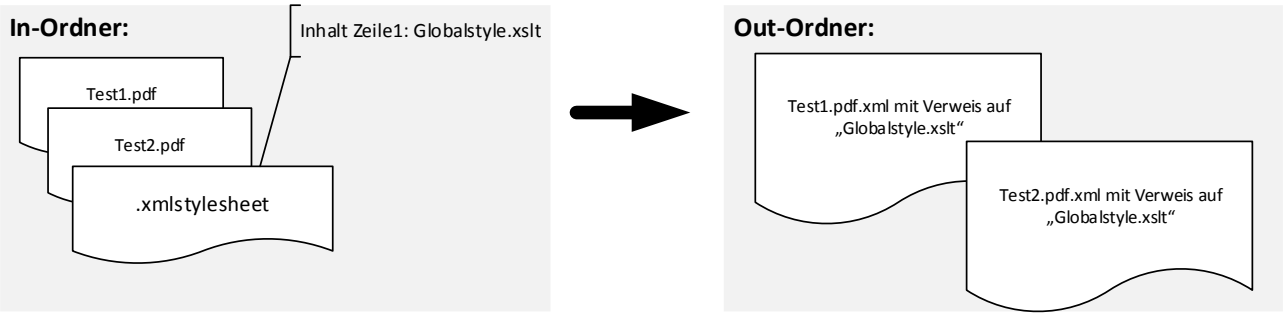
jedoch ein eigenes Stylesheet für das generierte XML benutzen, so muss man den Dateinamen der XSLT-Datei mit in das IN-Verzeichnis übertragen.

Hierbei gibt es zwei Möglichkeiten:

1. Die XSLT-Datei heisst entsprechend der zu verifizierenden Datei, dann werden diese Dateien zusammen verarbeitet



2. DIE XSLT-Datei beginnt mit einem Punkt, ist also namenlos und gilt damit für alle eingelieferten Dokumente



4.2.3 Verifikation

Unter Einstellungen/Verifikation können Sie die Mechanismen der Signaturprüfung bestimmen, welche verwendet werden sollen

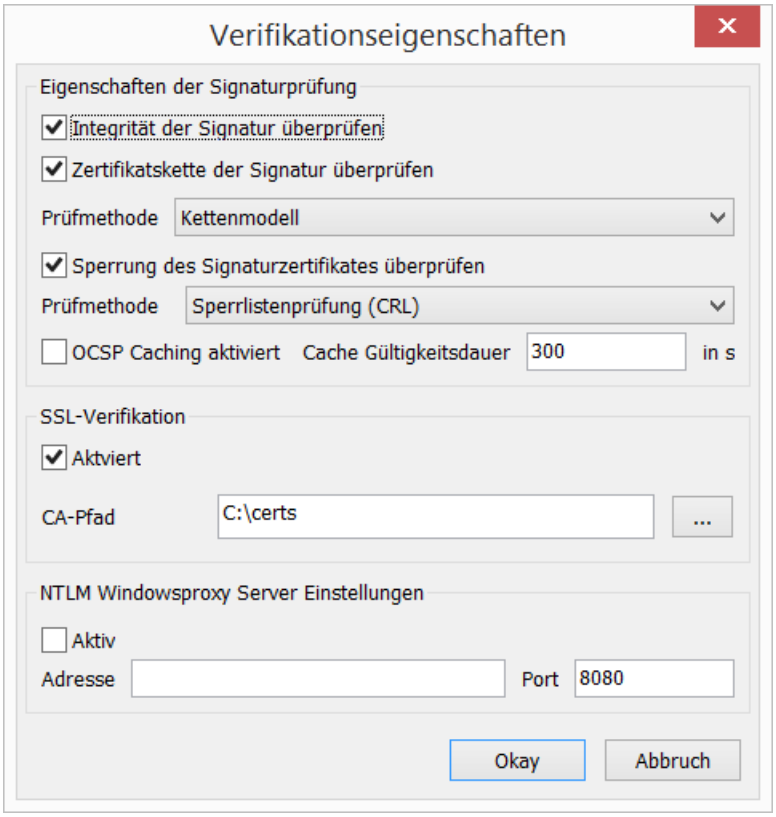


Abbildung 4-20 Verifikationseigenschaften

Eigenschaften der Signaturprüfung

Integrität der Signatur überprüfen

Mit der Integrität wird in diesem Zusammenhang die Unversehrtheit der Datei geprüft. Es wird ein Hashwert der Datei gebildet und dieser wird mit dem Hashwert verglichen, welcher in der Signatur hinterlegt wurde.

Zertifikatskette der Signatur überprüfen

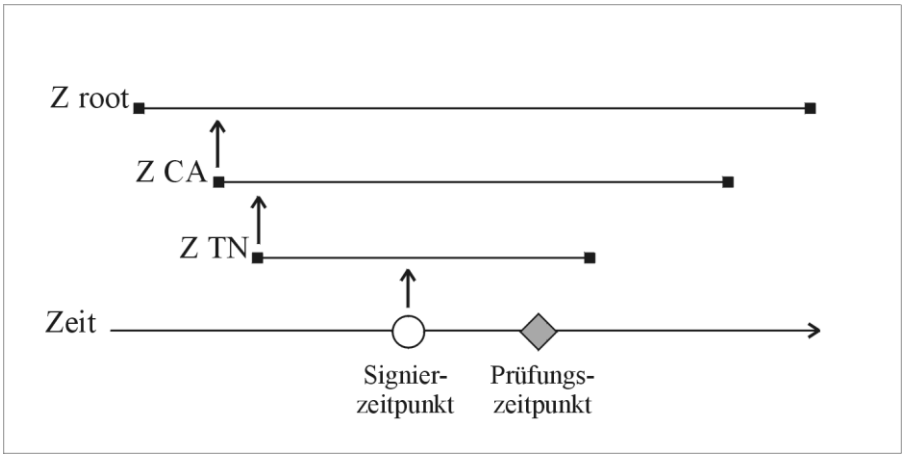
Damit ein Zertifikat überprüft werden kann, enthält dieses eine Verweis auf das Zertifikat der Zertifizierungsstelle, die das Zertifikat ausgestellt hat. Technisch gesprochen handelt es sich bei diesen Verweisen um eine digitale Signatur (Unterschrift) der Zertifizierungsstelle. Die Anwendungsprogramme können mit dem Zertifikat der Zertifizierungsstelle die Gültigkeit eines Zertifikates zu überprüfen.

Aus technischen oder organisatorischen Gründen, kann es sein, dass das Zertifikat einer Zertifizierungsinstanz seinerseits wieder einen Verweis auf ein Zertifikat einer übergeordneten Zertifizierungsinstanz enthält.

Auf diese Weise hat man eine Kette oder eine Hierarchie von Zertifikaten, die überprüft werden müssen, um die Gültigkeit eines Zertifikats zu überprüfen.

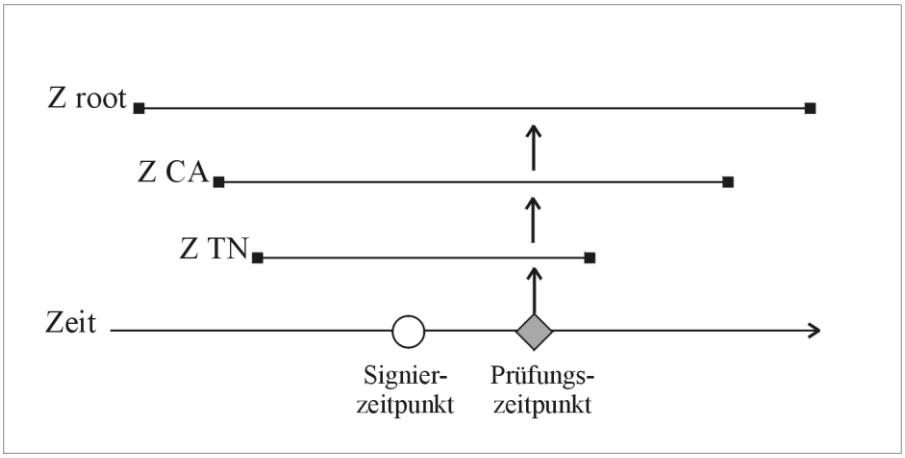
Prüfmethode

- Kettenmodell
  Das Kettenmodell (Verifikation zum Signierzeitpunkt) hat schwächere Kriterien, ein Zertifikat als gültig zu bewerten. Es wird nur gefordert, daß jedes Zertifikat im Zeitpunkt seiner Anwendung gültig war. Das bedeutet: zum Signierzeitpunkt des Dokuments muß das Teilnehmer-Zertifikat ZTN gültig gewesen sein. Zum Zeitpunkt der Zertifizierung desTeilnehmer-Zertifikates muß das CA-Zertifikat ZCA gültig gewesen sein usw.



  Ob ein Zertifikat seit der Dokumentsignatur gesperrt wurde, bleibt in diesem Modell unberücksichtigt.

- Schalenmodell
  Dieses Gültigkeitsmodell wird im PEM-Standard [RFC 1421-1424] beschrieben. Die Gültigkeit von Schlüsseln und Zertifikaten ist gemäß RFC1422 wie folgt definiert:
  * Ein Schlüssel(-paar) ist zu einem bestimmten Zeitpunkt genau dann gültig, wenn zu diesem Zeitpunkt der zugehörige Zertifizierungspfad gültig ist.
  * Ein Zertifizierungspfad ist zu einem bestimmten Zeitpunkt ganau dann gültig, wenn alle in ihm enthaltenen Zertifikate zu diesem Zeitpunkt gültig sind.
  * Ein Zertifikat ist zu einem bestimmten Zeitpunkt genau dann gültig, wenn
    - die Signatur des Zertifikates gültig ist.
    - der fragliche Zeitpunkt innerhalb des Gültigkeitszeitraums des Zertifikates liegt.
    - das Zertifikat nicht in der zum Zeitpunkt der Prüfung aktuellen Sperrliste der ausstellenden Zertifizierungsstelle enthalten ist oder das Zertifikat enthalten ist, der angegebene Sperrzeitpunkt jedoch nach dem fraglichen Zeitpunkt liegt.



Sperrung des Signaturzertifikates überprüfen

Jede CA führt eine Sperrliste (certificate revocation list (CRL)), auf die mit Hilfe des Verzeichnisdienstes alle Teilnehmer Zugriff haben. Hier werden alle zurückgenommenen Zertifikate (anhand der Seriennummer) mit einem Rücknahmedatum abgespeichert. Im AutoVerifier DCE kann eingestellt werden, auf welche Art die Sperrung geprüft wird. Mögliche Vorgänge sind:

- OCSP-Responder abfragen
- Sperrlistenprüfrung (CRL)

OCSP-Caching an/aus + Cache Gültigkeitsdauer

Um bei jeder Verifikation eine eigene OCSP-Anfrage zu vermeiden, kann das OCSP-Caching eingeschaltet werden. Zusammen mit der Gültigkeitsdauer in Sekunden kann hier eingestellt werden, ob eine erneute Abfrage gestartet wird, oder ob das Ergebnis der letzten OCSP-Abfrage aus dem Zwischenspeicher herangezogen wird.

SSL-Verifikation

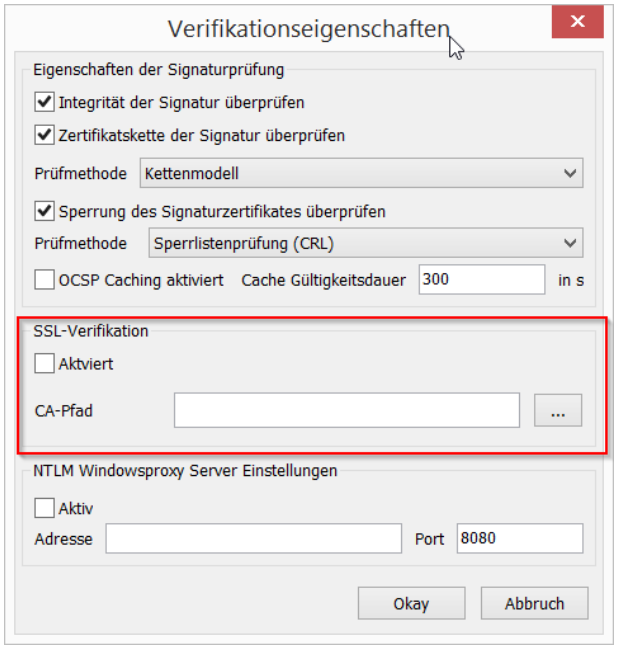


Abbildung 4-21 SSL-Verifikationseinstellungen

Statt dem Windows-Zertifikatsspeicher kann für die Verifiaktion ein Verzeichniss mit den entsprechenden Zertifikaten (via openssl) benutzt werden. Hierfür kann dieser Verifikationstyp aktiviert werden. Falls aktiviert, muss auch das Verzeichnis zu den CA-Zertifikaten angegeben werden.

NTLM Windowsproxy Server Einstellungen

NTLM (kurz für NT LAN Manager) ist ein Authentifizierungsverfahren für Rechnernetze. Es verwendet eine Challenge-Response-Authentifizierung.

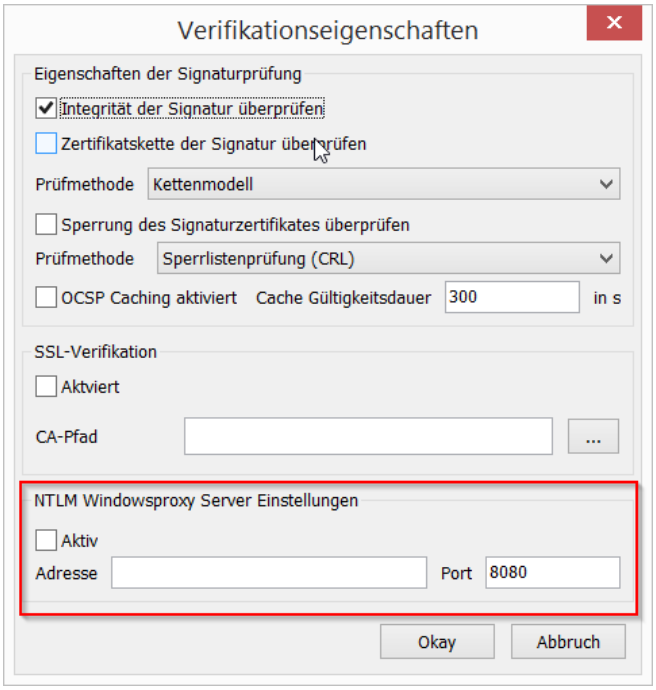


Abbildung 4-22 NTLM-Einstellungen

Durch den Einsatz von NTLM über HTTP ist ein Single Sign-on auf Webservern oder Proxyservern unter Verwendung des Berechtigungsnachweises (Credentials) der Windows-Benutzeranmeldung möglich.

Generell kann die Benutzung des NTLM-Windowsproxy aktiviert bzw. deaktiviert werden.

Für die korrekte Funktion muss die Adresse, sowie der Port des Authentifizierungssservers eingetragen werden.

4.2.4 OCSP-Responder

Das Online Certificate Status Protocol (OCSP) ist ein Netzwerkprotokoll, das es Clients ermöglicht, den Status von X.509-Zertifikaten bei einem Validierungsdienst abzufragen.

In der Regel sind die OCSP-Resonderdaten im Zertifikat enthalten. Dies kann man bei Zertifikaten im Zertifikatsspeicher direkt kontrollieren:

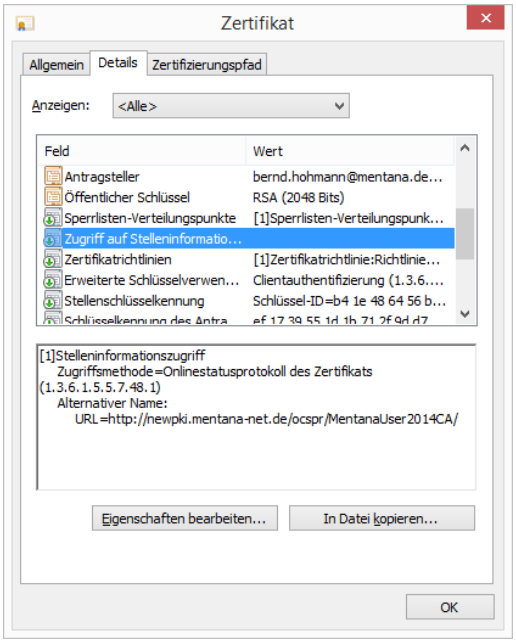


Abbildung 4-23 Anzeige Zertifikat mit OCSP-Daten

Der AV DCE entnimmt diese Daten der zu prüfenden Unterschrift auf der Eingangsdatei. Wenn aber keine OCSP-Daten vorhanden sind, bzw. wenn die enthaltene URL falsch oder nicht mehr erreichbar ist, würde eine Verifikation fehlschlagen.

Daher kann man dem AV DCE für bestimmte Zertifikate entsprechende OCSP-Responder mitteilen. Hierzu muss man den Zertifikatsherausgeber und die Seriennummer des Zertifikats wissen (bzw. keine Nr angeben für alle Zertifikate des Herausgebers).

Über Einstellungen / OCSP-Responder können Sie die OCSP-Responder konfigurieren

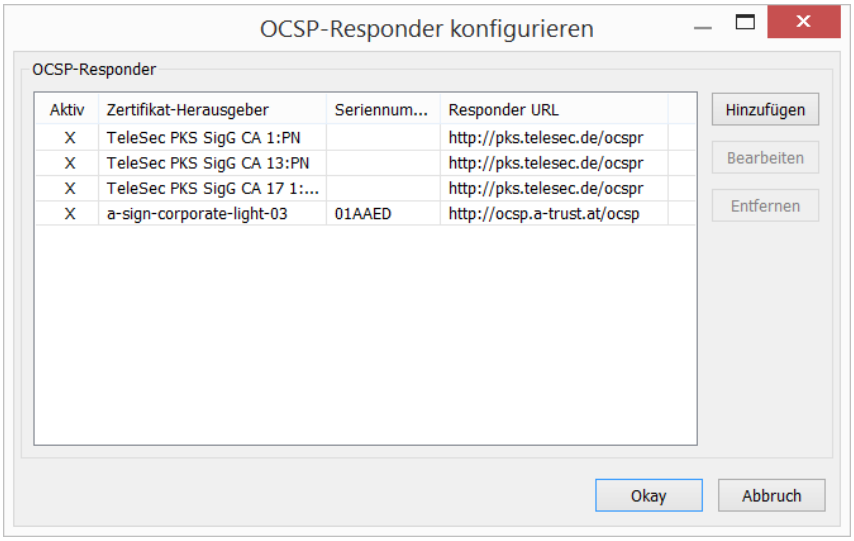


Abbildung 4-24: OCSP-Responder

OCSP-Resonder können hinzugefügt, bearbeitet oder entfernt werden. Für neue OCSP-Resonder, müssen folgende Parameter eingetragen werden:

Abbildung 4-25 Eigenschaften OCSP-Responder

Wählt man „Bearbeiten" aus, so kann man die entsprechenden Daten korrigieren.

Abbildung 4-26 Einschaften OCSP-Responder Beispieldaten

Beispielsweise kann man die URL ändern, oder auch die Verwendung des Responders deaktivieren.

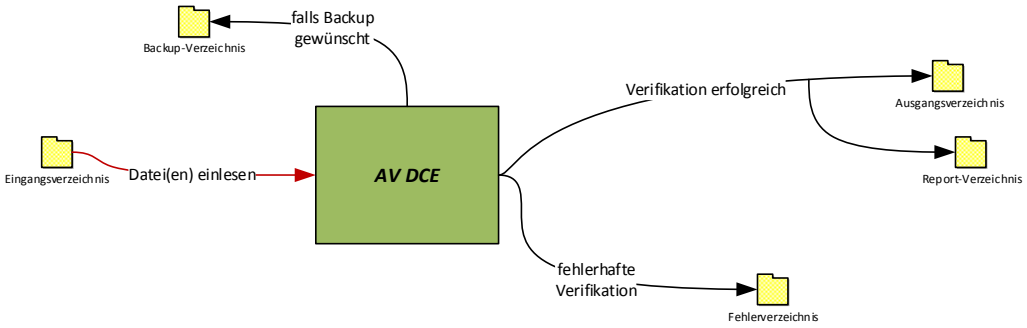
Im oben gezeigten Beispiel wird ein Zertifikat mit der Seriennr „01AAED" vom Herausgeber „a-sign-corporate-light-03" gegen die URL http://ocsp.a-trust.at/ocsp getestet.

Zertifikate vom Herausgeber „TeleSec PKS SigG CA 17 1:PN" werden alle gegen die OCSP-URL http://pks.telesec.de/ocspr getestet.

4.2.5 Verzeichnisüberwachung

Nachdem Sie über Einstellungen / Verzeichnisüberwachung in die Verzeichnisauswahl gelangt sind, können dort die unterschiedlichen Pfadangaben je nach Verwendungszwecke geändert werden.

4.2.5.1 Verzeichnisse



Verzeichnisse

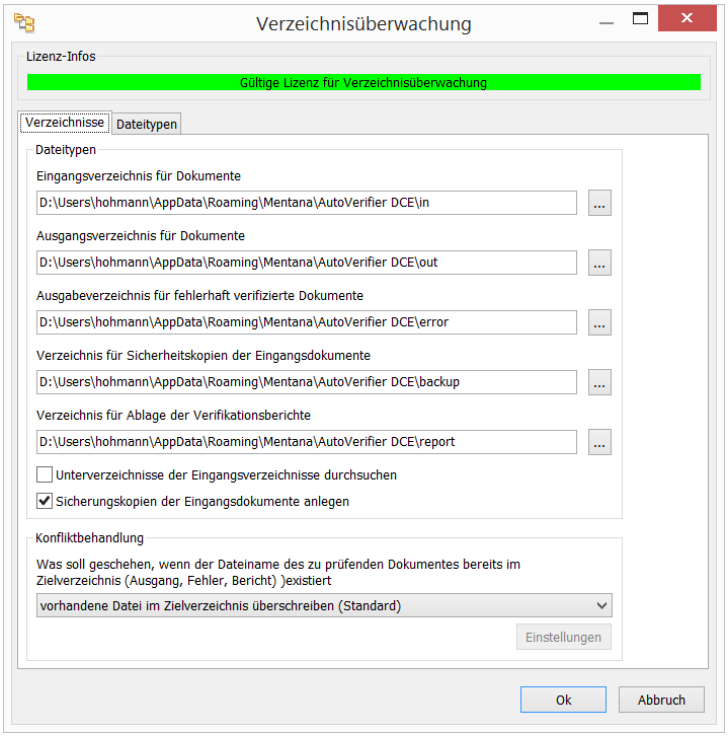


Abbildung 4-27 Dialog zur Festlegung der Verzeichnisse

Die folgenden Pfadangaben sind festzulegen:

- *Eingangsverzeichnis*: Eingangsverzeichnis für die zu verifizierenden Dokumente.
- *Ausgangsverzeichnis*: Ausgangsverzeichnis für die erfolgreich verifizierten Dokumente.
- *Fehlerverzeichnis*: Verzeichnis für fehlerhaft oder nicht verifizierte Dokumente.
- *Sicherungsverzeichnis*: Verzeichnis für Sicherungskopien der Eingangsdokumente.
- *Verifikationsprotokollverzeichnis*: Verzeichnis für die Ergebnisdateien (Protokolle) der Verifikation.

Die Verzeichnisse können direkt in die Eingabefelder eingegeben oder über einen „Ordner suchen" Dialog ausgewählt werden, der nach Anklicken des entsprechenden Buttons rechts neben dem Eingabefeld erscheint.

Es ist zu beachten, dass nur existierende Verzeichnisse bei der direkten Eingabe akzeptiert werden. Andernfalls wird eine Fehlermeldung angezeigt und der ursprüngliche Wert wieder hergestellt.

Konfliktbehandlung

Im Abschnitt Konfliktbehandlung konnen Sie festlegen, wass passieren soll, wenn der Dateiname der zu prüfende Datei in einem der oben konfigurierten Zielverzeichnisse vorhanden ist. Es gibt folgende Möglichkeiten:

- Vorhandene Datei im Zielverzeichnis überschreiben (standard).
- Zu prüfende Datei überspringen.
- Zu prüfende Datei umbenennen, sodass der Dateiname eindeutig wird.

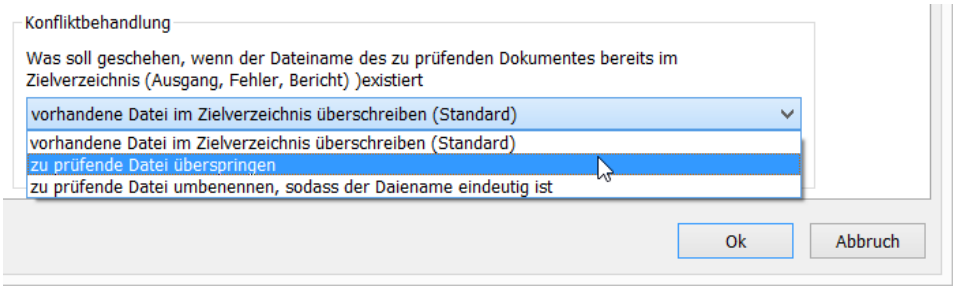


Abbildung 4-28 Konfliktbehandlung

In den letzten beiden Fällen gibt es weitere Konfigurationsmöglichkieten (Abbildung 4-29 und Abbildung 4-30).

Überspringen von Dateien

Wenn die Konfliktbehandlung so konfiguriert wurde, dass Dateien übersprungen werden, die in einem Zielverzeichnis vorhanden sind, kann in diesem Falle eine Semaphoren-Datei (Skip-Datei) erstellt werden. Das hat den Vorteil, dass beim nächsten Durchsuchen des Eingangsverzeichnises Dateien mit einer Semaphoren-Datei (Skip-Datei) gleich ignoriert werden. Erst wenn die Semaphoren-Dateien gelöscht werden, erfolgt eine erneute Verifikation dieser Dateien.

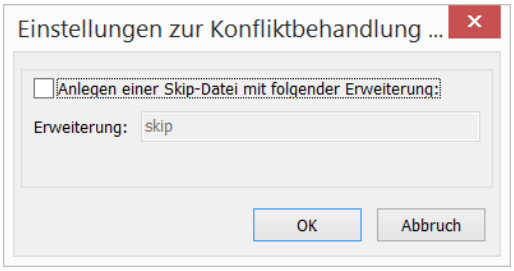


Abbildung 4-29: Dialog zur Festlegung des Verhaltens beim Überspringen von Dateien

Ist das Überspringen von Dateien wie in der Abbildung konfiguriert und ist der Name der zu prüfende Datei `Dokument.pdf` im Ausgansverzeichnis bereits vorhanden so wird im Eingangsverzeichnis die Semaphoren-Datei `Dokument.pdf.skip` mit leerem Inhalt angelegt. An diesen Dateien kann man erkennen, dass der AV DCE die dazu passende Datei überspringt.

Umbenennen von Dateien

Ist die Konfliktbehandlung auf „Datei umbenennen“ konfiguriert, kann festgelegt werden, wie das Umbenennen erfolgen soll.

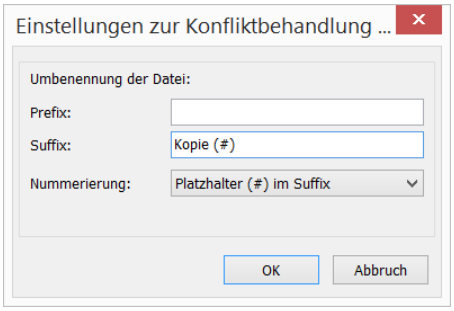


Abbildung 4-30: Dialog zum Festlegen des Verhaltens beim Umbenennen von Dateien

Die Datei wird mit Hilfe eines Prefixes, Suffixes und einer fortlaufenden Nummer solange umbenannt, bis der Dateiname in allen Zeilverzeichnissen eindeutig ist. Die Position der fortlaufenden kommer kann wie folgt festgelegt werden:

- Nach dem Suffix.
- Nach dem Prefix.
- Platzhalter (#) im Suffix
- Platzhalter (#) im Prefix

Als Standart wird die laufende Nummer an den Suffix angehängt. Bei Verwendung einer Einstellung mit dem Platzhalter ‚#' wird dieser durch die laufende Nummer ersetzt.

Bei der Einstellung aus Abbildung 4-30 würde die Datei

`Dokument.pdf` in `Dokument Kopie (1).pdf`

umbenannt, wenn es im Ausgangsverzeichnis eine Datei mit Namen `Dokument.pdf` gibt. Sollte die umbenannte Datei `Dokument Kopie (1).pdf` im Ausgansverzeichnis auch schon existieren, wird sie in `Dokument Kopie (2).pdf` umbenannt, dann in `Dokument Kopie (3).pdf` usw. bis der Dateiname eindeutig ist. Erst nachdem ein eindeutiger Dateiname gefunden wurde, werden die Namen der Protokoll- und Ziel-Dateien (wie kofiguriert) gebildet.

4.2.5.2 Dateitypen

Unter Einstellungen / Verzeichnisüberwachung kann auf der Seite Dateitypen festgelegt werden, wie der AV DCE mit bestimmten Dateitypen umgehen soll.

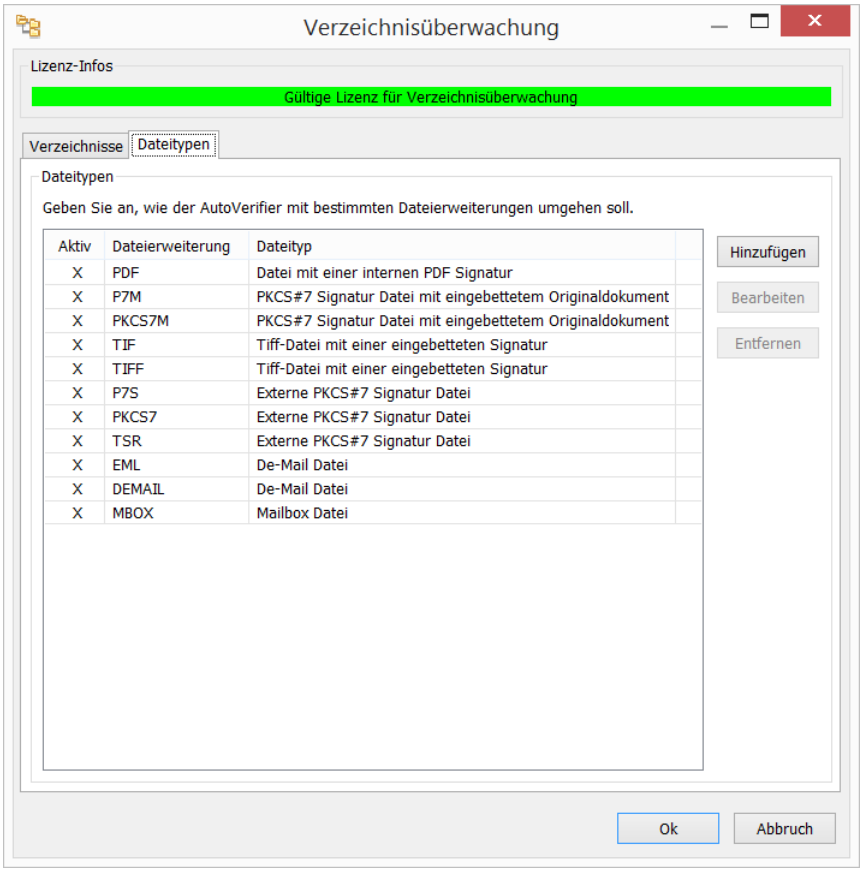


Abbildung 4-31: Dateierweiterungen

Bitte geben Sie die Dateierweiterungen in Großbuchstaben an. Jeder Erweitung weisen Sie einfach einen Dateityp zu.

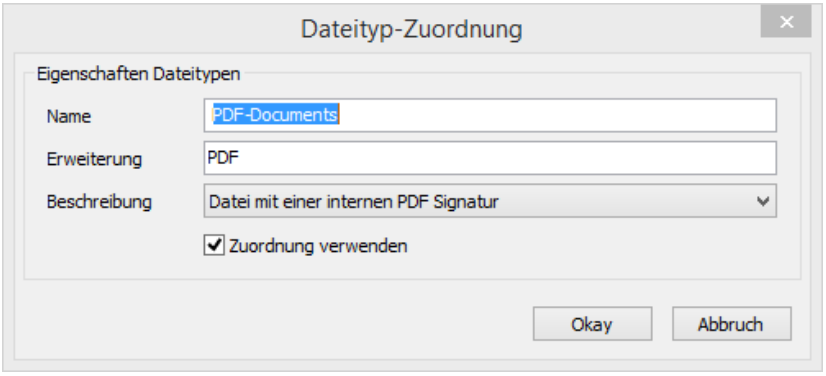


Abbildung 4-32 Dateitypen-Behandlung

Zur Auswahl stehen:

Anzeige Behandlung	Aktion des AV DCE
Datei wird ignoriert	Datei wird ignoriert
Datei mit einer internen PDF-Signatur	Signatur wird verifiziert
Externe PKCS#7 Signatur Datei	Signatur wird verifiziert
PKCS#7 Signatur Datei mit eingebettetem Originaldoklument	Signatur wird verifiziert
Tiff-Datei mit einer eingebetteten Signatur	Signatur wird verifiziert
Datei wird verschoben	Datei wird verschoben
De-Mail Datei	Datei wird als De-Mail[3] verifiziert
Mailbox Datei	Mailinhalt wird als De-Mails verifiziert

Dateien mit unbekannten Endungen werden vom AV DCE ignoriert.

Aktuell eingestellte Endungen – Aktionen

PDF	Datei mit einer internen PDF-Signatur/ Signatur wird verifiziert
P7M, PKCS7M	PKCS#7 Signatur Datei mit eingebettetem Originaldokument/ Signatur wird verifiziert
TIF, TIFF	Tiff-Datei mit einer eingebetteten Signatur/ Signatur wird verifiziert
P7S,PKCS7,TSR	Externe PKCS#7 Signatur Datei/ Signatur wird verifiziert
EML,DEMAIL	De-Mail Datei/ Datei wird als De-Mail verifiziert
MBOX	Mailbox-Datei/ Inhalt wird als De-Mails verifiziert

[3] De-Mail Version 1.0 und 1.1

Immer wenn der AV DCE gestartet wird, überprüft er diese Dateitypen und registriert die entsprechenden Aktionen. Im Log-File erfolgt eine Ausgabe. In der GUI wird das jeweils aktuellste Log-File angezeigt.

[]

4.2.6 SOAP-Connector (Zusatzmodul)

Einstellungen / Webservice-Konnektor öffnet ein Dialog um die Verbindungseinstellungen für die Webservice-Vorgangsdatenbank anzugeben. Diese Feature muss über die Lizenzdatei erlaubt sein, sonst haben die Einstellungen keine Auswirkungen.

Um diese Verbindung nutzen zu können, müssen Sie eine Verbindung zu einer AutoVerifier-Servicedatenbank herstellen. Die zum Zugriff auf die Vorgangsdatenbank verwendete DSN muss vorab erfolgreich konfiguriert sein (siehe Zusatzhandbuch).

Auf dem Einstellungsdialog tragen Sie den Namen der Datenquelle, sowie die Zugangsdaten aus und betätigen die Schaltfläche Verbindung testen. Nachdem der AutoVerifier den erfolgreichen Test der Datenbank-Verbindung bestätigt hat, können Sie unter Dienst einen verbundenen SOAP-Connector auswählen.

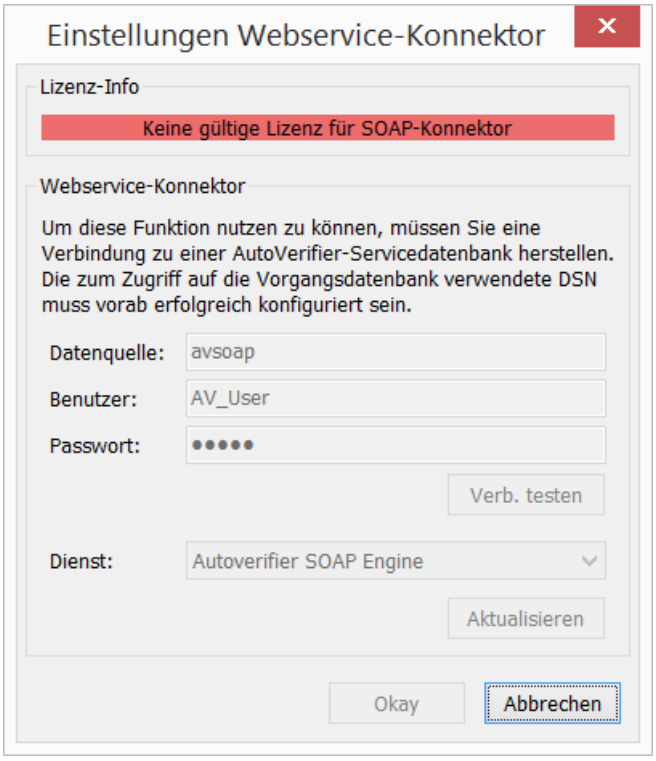


Abbildung 4-33 Einrichten Verbindungsdatenbank

Anschließend können Sie unter Einstellungen / Allgemein auf den Betriebsmodus „SOAP-Schnittstelle“ umschalten.

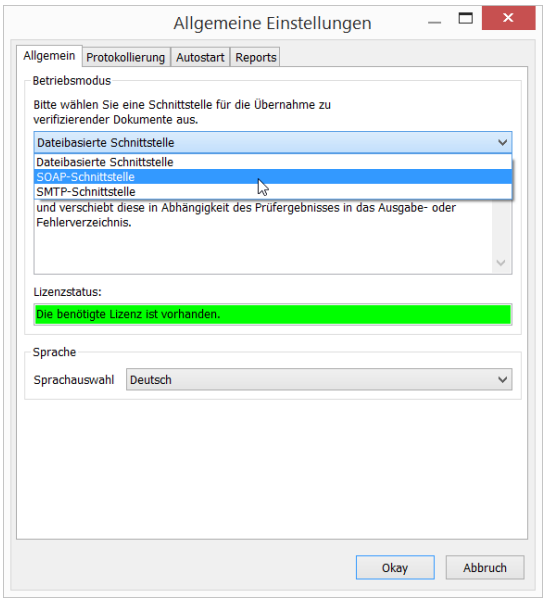


Abbildung 4-34 Betriebsmodus SOAP-Connector

Beim nächsten Start des Verifikationsvorganges stellt der AutoVerifier die Verbindung zum SOAP-Connector automatisch her.

4.2.7 Remote-Konsole

Unter „Einstellungen → Remoteconsole“ können sie die sog. Remote-Konsole konfigurieren.

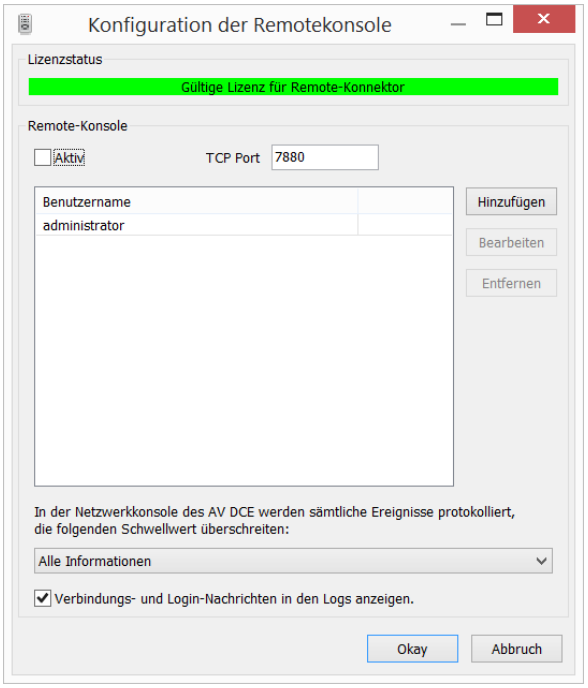


Abbildung 4-35: Remoteconsole konfigurieren

Mit der Remote-Konsole können Sie die Steuerung des AV DCE mit telnet übernehmen. Sobald Sie

- einen Benutzernamen mit Passwort erstellt haben
- einen Port eingetragen haben
- die Konsole aktiv geschaltet haben
- den AV DCE anschließend neu gestartet haben

können Sie via telenet die Steuerung vornehmen.

Beim Startem des AV DCE kann es zu einer Meldung der Firewall kommen, diese muss von Ihnen mit „Zugriff zulassen“ quittiert werden.

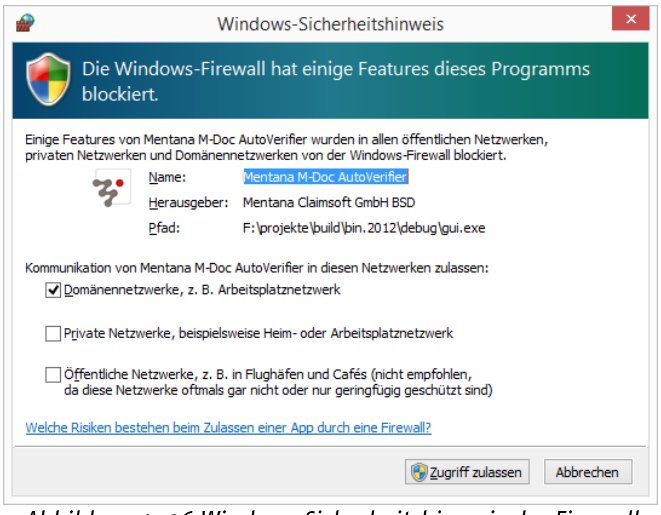


Abbildung 4-36 Windows Sicherheitshinweis der Firewall

Mittels Befehl
`telnet localhost 7880`
können Sie die Konsole auf dem Rechner testen, wo auch der AV DCE läuft:

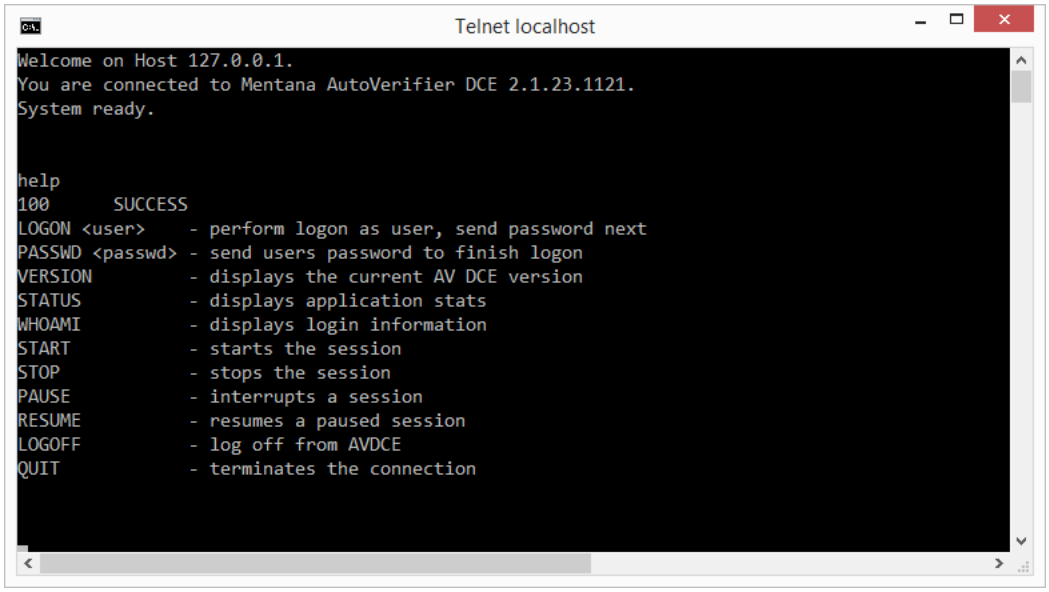


Abbildung 4-37 Kommandozeile mit gestartetem Telnet-Zugriff

Folgende Befehle stehen Ihnen über die Konsole zur Verfügung

Befehl	Bedeutung
HELP	Anzeige aller möglichen Befehle
LOGON	Als Benutzer einloggen, als nächstes muss das Passwort gesendet warden
PASSWD	Abschicken des Passwortes, um den Anmeldevorgang abzuschließen
VERSION	Die aktuelle Version des AV DCE wird angezeigt.
STATUS	Der aktuelle Status wird angezeigt: STATUS 3 STATUS-MSG STOPPED TOTAL 0 SUCCESS 0 FAILED 0 ACTIVE-SINCE INSTANCE-NAME Mentana AutoVerifier DCE
WHOAMI	Die Login-Informationen werden angezeigt
START	Die Verifikation wird gestartet.
STOP	Die Verifikation wird gestoppt.
PAUSE	Die Verifikation wurde angehalten.
RESUME	Die Verifikation wird wieder gestartet.
LOGOFF	Der Benutzer wird vom AV DCE ausgeloggt.
QUIT	Die Verbindung wird beendet

Wenn man in der Konfiguration Connect und Loggin in den Nachrichten anzeigen aktiviert, bekommt man in der Ereignisanzeige eine entsprechende Meldung, wenn sich jemand über die Remote-Konsole zuschaltet,

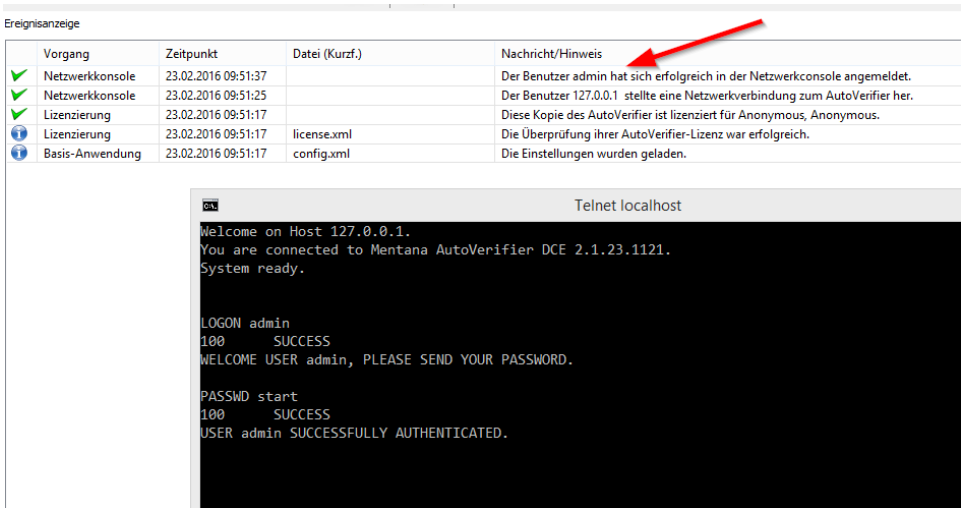


Abbildung 4-38 Einloggen und Log-Meldung

4.2.8 Werkzeuge

4.2.8.1 Liste leeren

Mit diesem Menüpunkt wird die Liste der angezeigten Ereignisse in der GUI geleert.

4.2.8.2 Statistik

Eine kurze Statistik über die durchgeführten Arbeiten des AV DCE wird angezeigt.

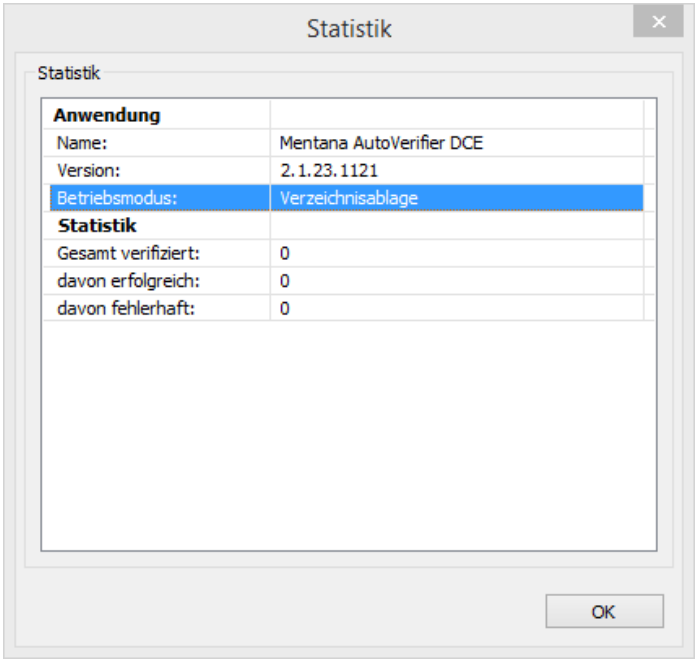


Abbildung 4-39 Statistik

4.2.8.3 Anzeige

Unter dem Menüpunkt Anzeige kann man die Oberfläche des AV DCE konfigurieren.

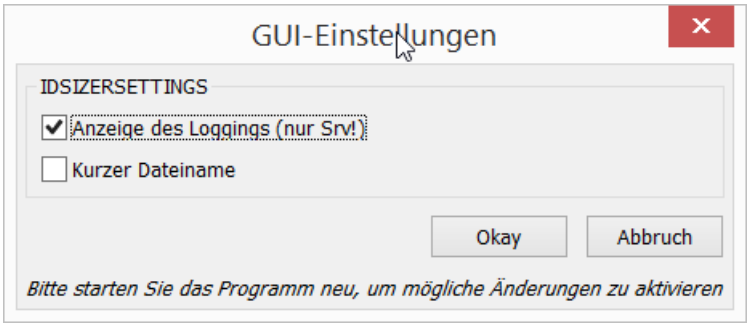


Abbildung 4-40 GUI-Einstellungen

AV-Programmart

Hier kann zwischen Standalone und Dienst gewählt werden, sofern die Lizenz dies erlaubt. Auf welche Art sich die Anzeige verändert, kann im Kapitel 4 nachgelesen werden.

Anzeige des internen Loggings

Läuft der AV DCE im Dienst-Modus, kann bei aktivierter Anzeige das Log des Dienstes im unteren Fensterbereich angezeigt werden.

Läuft der AV DCE im Standalone-Modus, erfolgt keine Log-Anzeige. Es sei denn, der AV DCE läuft im sog. Debug-Modus. Dann werden im unteren Bereich sog. Debug-Logs angezeigt.

Kurzer Dateiname

In der Ereignisanzeige erfolgt die Auflistung von Vorgang, Zeitpunkt, Datei und Nachricht in jeweils einer Spalte. Für die Spalte „Nachricht" kann angegeben werden, ob hier nur der Dateiname oder der ganze Pfad der Datei angezeigt wird.

4.2.8.4 Dienste

Wählt man diesen Programmpunkt aus, durchsucht das programm die installierten Dienste auf dem aktuellen Computer und zeigt alle AV DCE-Dienste an.

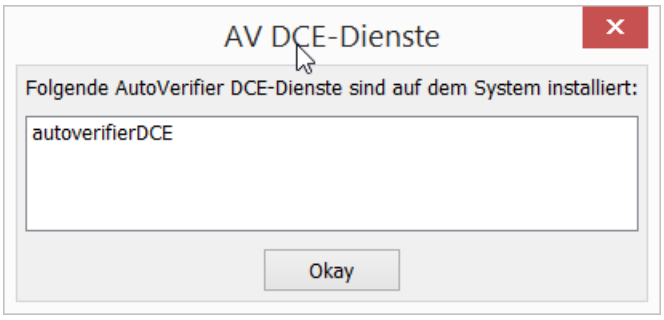


Abbildung 4-41 AV DCE-Dienste Auflistung

4.2.9 Hilfe

4.2.9.1 Über Mentana AutoVerifier

Unter dem Menüpunkt Hilfe kann der Kontakt zum Support aufgebaut werden. Weiterhin gelangt man hier zu einem Info-Fenster über den AV DCE.

Abbildung 4-42 Info-Fenster

4.3 DCE-Webkonsole

Für die Steuerung des AV DCE gibt es als Add-On die sog. DCE Webkonsole. Dies ist ein separates Produkt und ist bei Mentana Claimsoft GmbH erhältlich. Sie ermöglicht die Steuerung über einen Internetbrowser.

4.4 Konfigurationsdatei

4.4.1 Server

Bei jedem Start des AutoVerifier Data Center Edition werden die Initialisierungsparameter aus der Konfigurationsdatei „config.xml“ eingelesen. Eine Beispieldatei befindet sich im Anhang. Mit dem Setup wird der Service mit folgender Einstellung installiert:

-h=“ C:\ProgramData\Mentana\AutoVerifier DCE\config.xml“

Damit wird die Konfigurationsdatei aus dem Verzeichnis

```
C:\ProgramData\Mentana\AutoVerifier DCE
```

genommen.

4.4.2 AV DCE GUI

Eine eigene Konfigurationsdatei für die GUI extistiert nicht. Zur Konfiguration der Datei des Servers muss die GUI entsprechend gestartet werden. Dazu kann mit –c="xxx" die Konfigurationsdatei gewählt werden, in welche die GUI die Daten schreibt. Der Name kann hierbei frei gewählt werden, wobei aber Sonderzeichen eventuell zu Problemen führen können und entsprechend vermieden werden sollte. UNC-Pfade sollte wie folgt angegeben werden: -configfile="[UNC-Pfad]" oder -c="[UNC-Pfad]". Idealerweise sollte diese Datei der Konfigurationsdatei des Services entsprechen.

Diese Datei wird geändert, wenn man mit der GUI Konfigurationswerte ändert.

Gibt man der GUI keine Konfigurationsdatei mit, so kann sich die GUI die Konfigurationsdatei auch aus den Dienst-Einstellungen holen (wenn man die GUI als Administrator startet). Ohne diese Sonderrechte können die Dienste nicht durchsucht werden. Damit gibt es eine Konfigurationsdatei und die GUI kann nicht gestartet werden.

Sollten mehrere Dienste installiert sein, so öffnet sich ein Auswahlfenster. Nachdem man den zu konfigurierenden Dienst ausgesucht hat, „holt" sich die GUI die entsprechende Datei.

5 KONFIGURATION

Für den reibungslosen Betrieb müssen zuerst einige Konfigurationen vorgenommen werden. Dies kann entweder über die GUI durchgeführt werden, oder direkt über die Konfigurationsdatei (s.u.)

Konfiguriert werden muss:

- Art der Schnittstelle, wie der AV DCE verwendet warden soll
- Verzeichnisse (bei Verwendung der Dateisystemschnittstelle), bzw. DB-Zugangsdaten bei SOAP oder SMTP-Modus
- Art der Reports der Verifikation (XML/PDF/Collection/ Zeitstempel)

5.1 Konfig mit der AV DCE-GUI

Vor dem ersten Verifikationsvorgang müssen einige Einstellungen vorgenommen werden. Mit der Installation des AV DCE wurde ein Icon bzw. ein Menüpunkt „Autoverifier DCE konfigurieren“ installiert. Öffnen Sie diesen und Sie gelangen zur AV DCE GUI (s.o.).

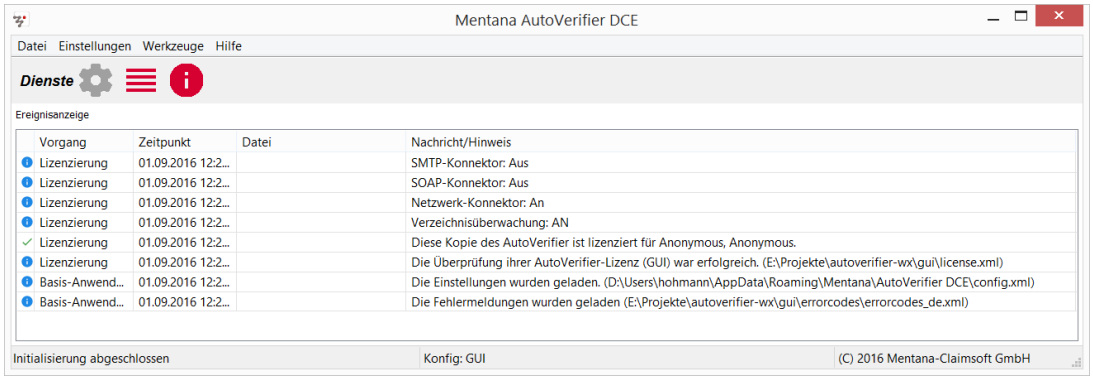


Abbildung 5-1 AV DCE Gui

Hier befindet sich im oberen Bereich das Menü des AV DCE. Darunter befindet sich je nach Konfiguration eine weitere Steuerungsleiste.

Im Menü ist der Menüpunkt Einstellungen hinterlegt.

Für die weiteren Einstellungen hängt es ab, in welchem Modus Sie den AV DCE betreiben wollen (s.u.) Nehmen Sie keine Einstellungen vor, so werden die Installationsstandardwerte verwendet.

Die Standardwerte oder die vorgenommenen Änderungen werden in einer Konfigurationsdatei „config.xml“ gespeichert.

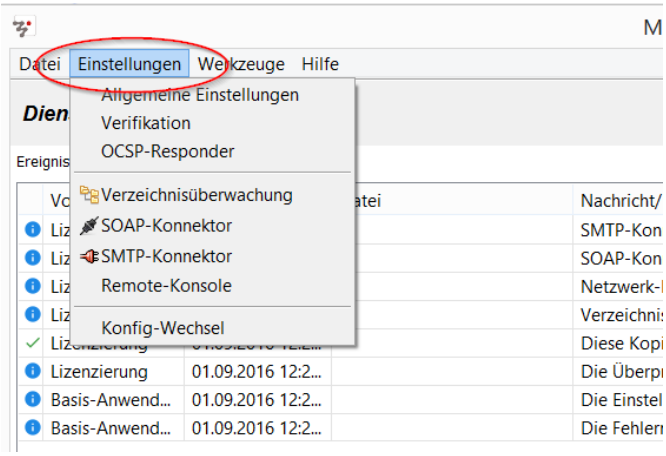


Abbildung 5-2 AutoVerifier DCE

5.2 Einstellungen direkt in der Konfigurationsdatei

Die Konfigurationsdatei config.xml ist eine normale XML-Datei, welche auch direkt mit einem Texteditor bearbeitet werden könnte.

Nachfolgend wird der Inhalt kurz erläutert:

5.2.1 GUI-Einstellungen

Im ersten Abschnitt der Konfigurationsdatei erfolgen die Einstellungen der GUI. Die hinterlegten Daten entsprechen dem Dialogfenster „GUI-Einstellungen" (siehe 4.2.8.3).

5.2.2 Anwendungsmodi

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

```
</gui>
<core>
    <operationmode>FILESTORE</operationmode>
```

Die Standardversion des AutoVerifier Data Center Edition stellt die Verwendung der Dateisystem-Schnittstelle zur Verfügung („FILESTORE"). Weitere mögliche Werte sind:

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

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

5.2.3 Sprache

Unter Language kann die aktuelle Sprache eingestellt werden.

```
<language>GERMAN</language>
<threadcount>5</threadcount>
```

Hier wird die verwendete Sprache hinterlegt. Möglich sind derzeit

- GERMAN
- ENGLISH

5.2.4 Prozessanzahl

Mit threadcount kann die Anzahl der maximalen Prozesse vom AV DCE eingestellt werden. Dies wird aktuell allerdings noch nicht vom AV DCE ausgewertet.

5.2.5 Logging

```
<logging>
    <threshold>
        <eventview>ALL</eventview>
        <email>FAILURE</email>
    </threshold>
    <emailsettings>
        <sendername/>
        <senderaddr/>
        <recipient/>
        <replyto/>
        <authrequired>true</authrequired>
        <server/>
        <user/>
        <passwd/>
        <digest>true</digest>
        <digestmode>DAILY</digestmode>
        <digestsize>10</digestsize>
    </emailsettings>
    <logger>
        <type>ROLLINGFILE</type>
        <location>C:\Users\Hohmann\AppData\Roaming\mentana\autoverifier\log</location>
    </logger>
</logging>
```

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

<Eventview> gibt hierbei den schwellwert für das interne Logging des AV DCE an.

<email> gibt an, welche Meldungen an den Admin gesendet werden werden.

Mögliche Werte sind hier für den Schwellwert:

- *INFORMATION*
  Alle Informationen
- *CRITICAL*
  Kritische Informationen
- *ERROR*
  Fehler
- *FATAL*
  Ausnahmefehler
- *ALL*
  alle Meldungen

Für das Versenden von Mailbenachrichtigungen müssen folgende Informationen eingetragen werden:

- *sendername*
  Absender-Name
- *senderaddr*
  Absender-Adresse
- *recipient*
  Empfänger-Adresse
- *replyto*
  Antwort-Adresse
- *server*
  Mailserver bzw. Mailprovider
- *user*
  Benutzername des Mailserver bzw. Mailprovider
- *passwd*
  Passwort für Mailserver bzw. Mailprovider

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

Mögliche Werte für den Typ sind

- ROLLINGFILE

5.2.6 Remoteconnector

Die Einstellungen für die Remotekonsole werden hier hinterlegt (siehe 4.2.7)

```
<remoteconnector>
    <activated>false</activated>
    <port>7880</port>
    <threshold>ALL</threshold>
    <showevents>false</showevents>
    <users>
        <user-account>
            <name>administrator</name>
            <password>changeoninstall</password>
        </user-account>
    </users>
</remoteconnector>
```

<activated> Gibt an, ob die Remotekonsole aktiviert ist

<port> Der TCP-Port

<threshold> Schwellwert der zu loggenden Ereignisse

<showevents> Verbindungs- und Login-Nachrichten in denLogs zeigen

<users> Hier sind die Remote-User hinterlegt mit <name> und <password>

5.2.7 Session

```
<session>
    <autostart>
        <active>false</active>
    </autostart>
</session>
```

<active> Hier wird angegeben, ob die Verifikationssitzung automatisch gestartet wird, wenn die GUI gestartet wird.

5.2.8 SSL-Verifikation

```
<ssl>
    <usage>false</usage>
    <capath>F:\Projekte\autoverifier-wx\gui\certs</capath>
    <cafile/>
</ssl>
```

<Usage> gibt an, ob dieses Vorgehen benutzt werden soll, oder nicht. Der **<capath>** Parameter gibt den Pfad zu den Zertifikaten an. **<cafile>** wird aktuell noch nicht ausgewertet.

5.2.8.1 Verifikationseigenschaften

Im Konfigurationsabschnitt **<verification>** werden die die Verifikationseinstellungen definiert.

```
<verification>
    <checkmode>
        <integrity>true</integrity>
        <name>false</name>
        <chain>true</chain>
        <time>true</time>
        <rev>true</rev>
    </checkmode>
```

<checkmode> steuert die Überprüfung der Verifikation nach der Verifizierung.

Hier können eingestellt werden:

<integrity> Überprüfung der Integrität einer Signatur

<name> Extraprüfung ob Name des Unterzeichners mit dem Namen im Signaturzertifikat übereinstimmt

<chain> Soll die Zertifikatskette der Signatur überprüft werden.

<time> Extraprüfung ob Zeitpunkt der Unterschrift im Gültigkeitszeitraum des Unterzeichnerzertifikats liegt

<rev> Überprüfung der Sperrung eines Signaturzertifikates

Der Abschnitt **<revocation>** legt fest, welche Signaturen für ungültig erklärt werden.

```
<revocation>
    <csp>false</csp>
    <x509>false</x509>
    <file>false</file>
    <ocsp>true</ocsp>
    <ldap>false</ldap>
    <http>false</http>
    <url/>
</revocation>
```

<csp> Sperrung überprüfen anhand der CRL-Datei

<x509> n/a

<file> n/a

<ldap> n/a

<ocsp> Sperrung überprüfen anhand des OCSP-Responder

<onlinetimeout> Timeout (in ms) für die OCSP-Anfragen.

Der Bereich OCSP-Caching beschreibt die OCSP-Einstellungen.

```
<ocspcaching>
    <activated>false</activated>
    <validity>300</validity>
</ocspcaching>
```

<activated> Caching aktiviert (true/false)

<validity> Gültigkeitsdauer Cache in s

lmntproxy beschreibt die Einstellungen für den NTLM-Windows-Proxy.

```
<lmntproxy>
    <activated>false</activated>
    <address/>
    <port>8080</port>
</lmntproxy>
```

<activated> Proxy an/aus

<address> Url des Proxys

<port> Port des aktuellen Proxys

Danach erfolgen die Einstellungen für die OCSP-Responder.

```
<ocspresponder>
    <responder>
        <issuer>TeleSec PKS SigG CA 1:PN</issuer>
        <serial/>
        <url>http://pks.telesec.de/ocspr</url>
        <activated>true</activated>
    </responder>
    <responder>
        <issuer>TeleSec PKS SigG CA 13:PN</issuer>
        <serial/>
        <url>http://pks.telesec.de/ocspr</url>
        <activated>true</activated>
    </responder>
    <responder>
        <issuer>TeleSec PKS SigG CA 17 1:PN</issuer>
        <serial/>
        <url>http://pks.telesec.de/ocspr</url>
        <activated>true</activated>
    </responder>
    <responder>
        <issuer>a-sign-corporate-light-03</issuer>
        <serial>01AAED</serial>
        <url>http://ocsp.a-trust.at/ocsp</url>
        <activated>true</activated>
    </responder>
</ocspresponder>
```

Anschließend werden die einzelnen Dateitypen definiert:

```
<filetypemap>
    <filetype>
        <description>PDF-Documents</description>
        <extension>PDF</extension>
        <action>PDF_DOCUMENT</action>
        <activated>true</activated>
    </filetype>
    <filetype>
        <description>Enveloped S/MIME</description>
        <extension>P7M</extension>
        <action>SMIME_ENVELOPED_SIGNATURE</action>
        <activated>true</activated>
    </filetype>
    <filetype>
        <description>Enveloped S/MIME</description>
        <extension>PKCS7M</extension>
        <action>SMIME_ENVELOPED_SIGNATURE</action>
        <activated>true</activated>
    </filetype>
    <filetype>
        <description>Signed TIFF-Documents</description>
        <extension>TIF</extension>
        <action>TIFF_DOCUMENT</action>
        <activated>true</activated>
```

5.2.9 Verifikationsmodus

```
                <activated>true<
            </filetype>
        </filetypemap>
        <mode>CHAIN</mode>
    </verification>
    <report>
```

Das Tag **<mode>** gibt die Prüfmethode der Verifikation an.

Mögliche Werte sind hier

- chain Kettenmodell
- shell Schalenmodell

5.2.9.1 Report

Im Konfigurationsabschnitt **<report>** wird u.a. das Verzeichnis für die Ablage der Verifikationsreporte sowie alle weiteren Einstellungen hinterlegt.

```
<report>
    <xml>
        <enabled>true</enabled>
        <prefix/>
        <suffix/>
        <stylesheet>http://www.mentana.de/verification/xsl/MentanaV3Result.xslt</stylesheet>
        <skipextension>false</skipextension>
    </xml>
    <pdf>
        <enabled>true</enabled>
        <prefix/>
        <suffix>_report</suffix>
        <stylesheet>E:\Projekte\autoverifier-wx\gui\stylesheet\mentana.xsl</stylesheet>
        <fophostname>localhost</fophostname>
        <fopport>1111</fopport>
        <skipextension>true</skipextension>
    </pdf>
    <collection>
        <enabled>false</enabled>
        <prefix/>
        <suffix>_package</suffix>
        <coversheet/>
        <skipextension>true</skipextension>
        <deletereport>false</deletereport>
        <showcoverpage>true</showcoverpage>
    </collection>
    <timestamp>
        <enabled>false</enabled>
        <serverurl>http://tsa.mentana-net.de/tsa/service</serverurl>
        <hashalgo>SHA-256</hashalgo>
    </timestamp>
</report>
```

5.2.10 Die Dateisystem-Schnittstelle

5.2.10.1 Anpassen der Arbeitsverzeichnisse

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

```
<filestoreengine>
    <folders>
        <in>D:\Users\hohmann\AppData\Roaming\Mentana\AutoVerifier DCE\in</in>
        <out>D:\Users\hohmann\AppData\Roaming\Mentana\AutoVerifier DCE\out</out>
        <backup>D:\Users\hohmann\AppData\Roaming\Mentana\AutoVerifier DCE\backup</backup>
        <report>D:\Users\hohmann\AppData\Roaming\Mentana\AutoVerifier DCE\report</report>
        <error>D:\Users\hohmann\AppData\Roaming\Mentana\AutoVerifier DCE\error</error>
    </folders>
    <behaviour>
```

- *in*
  Ordner, der auf zu verifizierende Dateien überprüft wird.
- *out*
  Ordner, der die verifizierten Dokumente enthält.
- *backup*
  Ordner, in dem Backups der Dokumente abgelegt werden.
- *report*
  Ordner, in dem Report Dateien abgelegt werden.
- *error*
  Ordner für die Dokumente, die nicht erfolgreich verifiziert wurden.

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

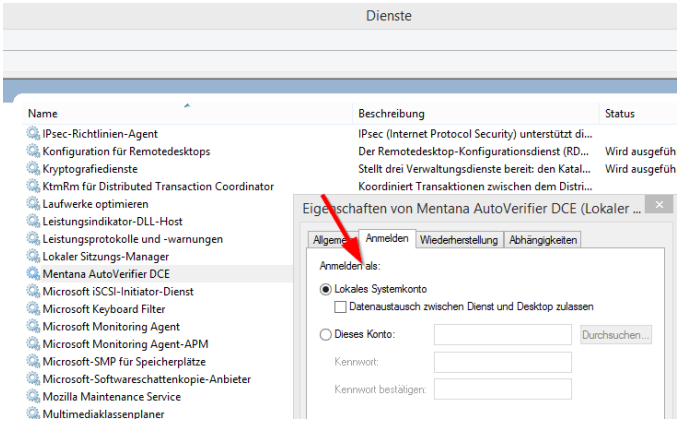


Abbildung 5-3 Dienste-Anzeige mit Eigenschaften/ Anmeldedaten

5.2.10.2 Dateihandling

Im Abschnitt **<behaviour>** können weitergehende Einstellungen bei der Verwendung der Dateisystem-Schnittstelle konfiguriert werden.

```
<behaviour>
    <sigfileextensions>pkcs7,p7s</sigfileextensions>
    <createbackup>true</createbackup>
    <scansubfolders>false</scansubfolders>
    <writeresult>false</writeresult>
</behaviour>
```

<createbackups> sollen im Backupverzeichnis Sicherheitskopien der zu verifizierenden Dokumente erstellt werden (true/false)

<scansubfolders> rekursives Abarbeiten des Eingangsordners (Unterverzeichnisse)

<writeresult> n/a

5.2.11 Soap Engine

Im Abschnitt **<soapengine>** werden die SOAP-Einstellungen konfiguriert.

```
<soapengine>
    <engine-id>1</engine-id>
    <queuedatabase>
        <dsn>avsoap</dsn>
        <user>AV_User</user>
        <password>start</password>
    </queuedatabase>
</soapengine>
```

5.2.12 SMTP-Engine

Einstellungen für die SMTP-Engine warden wie folgt konfiguriert:

```
<smtpengine>
    <engine-id>1</engine-id>
    <queuedatabase>
        <dsn>avsoap</dsn>
        <user>AV_User</user>
        <password>start</password>
    </queuedatabase>
</smtpengine>
```

6 LOG-AUSGABEN

Die erfolgreich durchgeführten Verifikationsvorgänge sowie Meldungen über aufgetretene Fehler werden in Logdateien mitgeschrieben. Die entsprechenden Meldungen werden in die jeweils aktuelle Logdatei geschrieben, wobei für jeden Tag eine neue Logdatei angelegt wird. Die Syntax des Dateinamens einer Logdatei lautet dabei *autoverifier-YYYY-MM-DD.log* (etwa autoverifier-2010-05-20.log).

Im Fenster Programm-Infos werden die aktuellen Log-Einstellungen angezeigt. Man kann dieses Fenster öffnen über das Menü Hilfe / Über das Programm, bzw. über die entsprechende Schaltfläche im Toolbar.

Abbildung 6-1 Icon Anzeige Info-Fenster

Das Info-Fenster wird angezeigt:

Abbildung 6-2 Info-Fenster mit markierten Log-Informationen

Im unteren Bereich werden die Daten für die Log-Möglichkeiten angezeigt.

Log-Art
Hier wird angezeigt, wohin vom AV DCE geloggt wird. Möglich ist derzeit

- RollingFile
- Database

Nähe Infos hierzu siehe Kapitel 4.2.2.3

Logging-Infos
In dieser Zeile wird angezeigt, in welchem Verzeichnis die Log-Dateien abgelegt werden. Dieser Ort kann über Einstellungen/ Allgemeine Einstellungen/ Seite Protokollierung eingestellt werden. In der Konfigurationsdatei `config.xml` befindet sich das Tag <logger> und darunter das Tag <location>. Hier wird der Pfad eingetragen:

Abbildung 6-3 Abschnitt in der Config.xml über Logging-Location

(Vgl. Kapitel 4.2.2.3)

Es können der Logdatei die nachfolgenden Informationen entnommen werden:

- Start des Verifikationsvorgangs nicht möglich → Ausgabe eines Fehlercodes (siehe 8.2.3)
- Info über den Start eines Verifikationsvorgangs.
- Welche Datei wurde verifiziert?
- Das Verifizieren einer Datei war erfolgreich oder ist fehlgeschlagen.
  → Ausgabe eines Fehlercodes (siehe 8.2.2).
- Abbruch des Verifikationsvorgangs
- Info über den Abschluss eines Verifikationsvorgangs.
- Weitere:
  - eine zu verifizierende Datei ist bereits im Ausgangsverzeichnis vorhanden.
  - der Schreibschutz einer Datei wurde entfernt.
  - eine Datei konnte nicht gelöscht werden.

Per Doppelklick auf diesen Eintrag wird die Log-Datei mit einem entsprechenden Programm, welches mit der Endung .Log verknüpft ist geöffnet. Es wird versucht, die LOG-Datei zum

aktuellen Datum zu öffnen. Ist diese nicht/ noch nicht vorhanden, wird das Verzeichnis im Datei-Explorer geöffnet und man bekommt alle vorhanden LOG-Dateien angezeigt.

API-Debug-Logging

Wird der AV DCE mit dem Parameter „`-l`“ gestartet, so wird zusätzlich ein internes Logging mitgeführt. Die dafür enthaltenen Konfigurationsoptionen befinden sich in der Datei `mentdbg.cfg`. Diese muss im Verzeichnis der Anwendung liegen. Sie enthält Angaben über die Art des internen Loggings der log4cxx-Komponente. Ist die Datei vorhanden und ist dort ein Eintrag für die Log-Datei vorhanden, so wird der Dateiname hier angezeigt. Auch hier kann mit Doppelklick die LOG-Datei geöffnet werden.

Service-Log

Sofern ein AV DCE Dienst vorhanden ist, wird in dessen Anwendungsverzeichnis nach dessen Konfigurationsdatei gesucht. Wurde diese gefunden und enthält diese Daten zum Logging, wird der entsprechenden Verzeichniseintrag ebenfalls angezeigt.
Per Doppelklick auf diesen Eintrag wird die Log-Datei mit einem entsprechenden Programm, welches mit der Endung .Log verknüpft ist geöffnet. Es wird versucht, die LOG-Datei zum aktuellen Datum zu öffnen. Ist diese nicht/ noch nicht vorhanden, wird das Verzeichnis im Datei-Explorer geöffnet und man bekommt alle vorhanden LOG-Dateien angezeigt.
Im Maus-Hinweistext wird zudem noch angezeigt, welche Konfigurationsdatei zum Service für diese Infos benutzt wurde.

7 ANHANG

7.1 PlugIns

7.1.1 SOAP-Connector/ SMTP-Connector

Hierbei handelt es sich um separat erhältliche PlugIns. Zusammen mit den PlugIns wird auch ein separates Handbuch geliefert.

7.2 Fehlercodes

Im Folgenden sind die möglichen Fehlercodes aufgelistet, die bei der Ausführung des AutoVerifier Data Center Edition innerhalb der Anwendung zurückgeliefert und in einer Logdatei ausgegeben werden.

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

Stand: 15.07.2016

allgmein

0	Operation erfolgreich abgeschlossen	INFO
1	Unbekannter oder nicht dokumentierter Fehler	INFO
-1	Datei konnte nicht geöffnet oder geschrieben werden	WARNING

Crypto-Fehler

-22	Fehlerhafte PKCS#7-Struktur.	FATAL
-24	Das Erstellen der kryptographischen Signatur schlug fehl.	FATAL
-27	Auf den privaten Schlüssel des Zertifikates konnte nicht zugegriffen werden.	FATAL
-28	Das ausgewählte Zertifikat ist nicht mehr verfügbar.	FATAL
-35	Dateiname des Dokumentes und der Signatur sind identisch.	FATAL
-36	Die Signaturdatei konnte nicht angelegt bzw. geschrieben werden.	FATAL
-58	Der zur Verarbeitung benötigte Speicher konnte nicht allokiert werden.	FATAL

Crypto-Middleware

-113	Keine Signatur in der Datei vorhanden.	ERROR
-114	Die PKCS#7-Struktur ist fehlerhaft oder nicht vorhanden.	ERROR
-115	Die PKCS#7-Struktur ist fehlerhaft oder nicht vorhanden.	FATAL
-117	Die PKCS#1-Struktur ist fehlerhaft oder nicht vorhanden.	ERROR
-118	Das Zertifikat einer PKCS#1-Signatur ist fehlerhaft oder nicht vorhanden.	ERROR
-200	Das Verschlüsseln schlug fehl, da das Zertifikat ungültig ist.	ERROR
-201	Das Verschlüsseln schlug fehl, da die Nachricht ungültig ist.	ERROR
-202	Das Verschlüsseln schlug fehl, da die erzeugte Nachricht ungültig ist.	ERROR
-203	Das Verschlüsseln des Dokumentes schlug fehl.	ERROR
-204	Das Entschlüsseln schlug fehl, da das Zert ungültig/ nicht vorhanden ist.	ERROR
-205	Das Entschlüsseln schlug fehl. Die verschlüsselte Nachricht konnte nicht verstanden werden.	ERROR
-206	Das Entschlüsseln schlug fehl. Das übergebene Dokument enthielt keine verschlüsselte Nachricht.	ERROR
-207	Das Entschlüsseln des Dokumentes schlug fehl.	ERROR
-300	ERROR_PKCS7_PREPARE	ERROR
-301	ERROR_PKCS7_OUTBUFFER	ERROR

PDF-API-Codes

-1001	Die PDF-Datei konnte nicht gelesen werden.	ERROr
-1002	Das Inhaltsverzeichnis des PDF-Dokumentes konnte nicht gelesen werden	ERROR
-1003	Die Position des PDF-Trailers konnte nicht ermittelt werden.	ERROR
-1004	Beim Lesen eines PDF-Datenfeldes trat ein Fehler auf.	ERROR
-1007	Die Größe des Dokuments verhindert eine Verarbeitung.	ERROR
-1008	Die Eingabedaten sind ungültig.	ERROR
-1012	Die Eingabedatei konnte nicht geöffnet werden.	ERROR
-1016	Das Auslesen eines PDF-Feldwertes schlug fehl.	WARNING
-1018	Der Trailer des PDF-Dokumentes konnte nicht gelesen werden.	ERROr
-1021	Das Dokument ist verschlüsselt und kann daher nicht signiert werden.	ERROR
-1022	Die sichtbare Signatur konnte nicht innerhalb der Seitenränder positioniert werden.	ERROR
-1023	Es konnte keine Instanz des signierten PDF-Dokumentes angelegt werden.	ERROR
-1025	Es wurde kein signaturfähiger Inhalt gefunden.	ERROR
-1026	Das Hinzufügen einer PDF-Anlage schlug fehl.	ERROR

-1027	Ein Objekt zur sichtbaren Unterschrifsdarstellung konnte nicht in das PDF-Dokument eingefügt werden.	ERROR
-1028	Die übergebene Grafikdatei konnte nicht geöffnet oder gelesen werden.	ERROR
-1029	Die übergebene Datei ist kein PDF-Dokument	ERROR
-1035	Das angegebene Hintergrundbild der Signatur ist nicht im JPEG-Format	ERROR
-1038	Das PDF-Dokument konnte nich angelegt oder geschrieben werden.	ERROR
-1040	Ein Datumsfeld hat ein inkorrektes Format.	ERROR
-1050	Die Seitengröße des Dokumentes konnte nicht ermittelt werden.	ERROR
-1081	Das Dokument konnte nicht gelesen werden.	ERROR
-1171	Das anzufügende Dokument konnte nicht geöffnet werden.	ERROR
-1172	Ein Datenblock konnte dem PDF-Dokument nicht hinzugefügt werden.	ERROR
-1173	Anhang konnte dem PDF-Dokument nicht hinzugefügt werden. Nicht unterstützter MIME-Typ.	ERROR
-1200	Das Durchsuchen des PDF-Dokumentes schlug fehl.	ERROR
-1801	Die Bestimmung der Signaturposition war nicht erfolgreich.	ERROR

MDoc APIExt-Error-Codes

8000	Die URL des Zeitstempeldienstes ist fehlerhaft.	ERROR
8001	Es konnte keine Verbindung zum Zeitstempeldienst hergestellt werden.	ERROR
8002	Der Gültigkeitszeitraum des Zertifikates ist beendet.	ERROR
8003	Bei der Verarbeitung ist ein schwerer Ausnahmefehler aufgetreten.	ERROR
8004	Innerhalb des CSP-Moduls ist eine Ausnahmesituation aufgetreten.	ERROR
8006	Im Dokument ist keine Signatur enthalten.	ERROR

MDocAPI Error-Codes

1	Die Zertifikatssperrliste wurde nicht gefunden.	FATAL
-1	Fehler beim Öffnen der CSP	FATAL
-2	Fehler beim Öffnen des Zertifikatsspeichers.	FATAL
-3	Fehler beim Schließen des Zertifikatsspeichers.	FATAL
-4	Fehler bei der Hashwertberechnung des Zertifikats.	FATAL
-5	Fehler beim Setzen der Version.	FATAL
-6	Fehler beim Setzten der CSP.	FATAL
-7	Fehler beim Setzten des Ausstellers.	FATAL
-8	Fehler beim Setzen der Seriennummer.	FATAL
-9	Fehler beim Setzen des Signaturalgorithmuses.	FATAL
-10	Fehler beim Setzen des Eigentümers.	FATAL
-11	Fehler beim Setzen der Eigentümer-Schlüssels.	FATAL
-12	Fehler beim Setzen des Eigentümer-Schlüssel-Atlgorithmuses.	FATAL
-13	Fehler beim Setzen des Gültigkeits-Bisdatum.	FATAL
-14	Fehler beim Setzen des Gültigkeits-Vondatum.	FATAL
-15	Fehler beim Setzen des Fingerabdruckes.	FATAL
-16	ERROR_CLOSING_CSP_AND_OPENING_CERTSTORE	FATAL
-17	ERROR_CLOSING_CSP_AND_CERTSTORE	FATAL
-18	ERROR_CLOSING_CSP	FATAL
-19	ERROR_SETTING_CERTCONTEXT	FATAL
-20	Kein Fingerabdruck vorhanden.	FATAL
-21	Falsche Person.	FATAL
-22	Fehlerhafte PKCS#7 Struktur.	FATAL
-23	XML Datei kann nicht geöffnet werden.	FATAL
-24	ERROR_BLOB_SIGN	FATAL
-25	ERROR_SETTING_NOTAFTERRAW	FATAL
-26	ERROR_SETTING_NOTBEFORERAW	FATAL
-27	ERROR_SETTING_DISPLAYNAME	FATAL
-28	ERROR_INVALID_CERTINDEX	FATAL
-29	ERROR_SIGN_FOR_LENGTH	FATAL
-30	ERROR_FAKE_HASH	FATAL
-31	ERROR_CERTSTORE_OPENSTORE	FATAL
-32	ERROR_CERTSTORE_ENUMCERT	FATAL

-33	ERROR_CERTSTORE_OPENCERT	FATAL
-34	Die PKCS#1-Struktur ist fehlerhaft oder nicht vorhanden.	FATAL
-35	Dateiname des Dokumentes und der Signatur sind identisch.	FATAL
-36	Die Signaturdatei konnte nicht angelegt bzw. geschrieben werden.	FATAL
-40	ERROR_SETTING_SCARD_INTERFACE	FATAL
-41	ERROR_SETTING_SCARD_CONTEXT	FATAL
-42	ERROR_SETTING_SCARD_CONNECT_CARD	FATAL
-43	ERROR_SETTING_SCARD_PKCS15_INIT	FATAL
-44	ERROR_SETTING_SCARD_CERT_ENUMERATION	FATAL
-45	ERROR_SETTING_SCARD_CERT_READ	FATAL
-46	ERROR_SETTING_SCARD_READER	FATAL
-50	ERROR_SETTING_SSLPKEYFILENAME	FATAL
-51	ERROR_SETTING_SSLCERTFILENAME	FATAL
-52	ERROR_SETTING_SSLPREFIX	FATAL
-53	ERROR_SETTING_SSLDIR	FATAL
-54	ERROR_CREATING_X509	FATAL
-55	ERROR_PARSE_X509	FATAL
-56	ERROR_SETTING_CERT_X509	FATAL
-57	ERROR_UNSUPPORTED_SIGNATURE_ALGO	FATAL
-58	Der zur Verarbeitung benötigte Speicher konnte nicht allokiert werden.	FATAL
-60	ERROR_INIT_PKCS11_ENGINE	FATAL
-71	ERROR_NO_READERS_FOUND	FATAL
-72	ERROR_WRONG_READER_SELECTED	FATAL
-73	ERROR_SMARTCARD_COMM_ERROR	FATAL
-74	ERROR_SMARTCARD_WRONG_CARD	FATAL
-75	ERROR_SC_WRONG_LEN_PW1	FATAL
-76	ERROR_SC_WRONG_LEN_PW2	FATAL
-77	ERROR_SC_WRONG_LEN_SIGPW1	FATAL
-78	ERROR_SC_WRONG_LEN_SIGPW2	FATAL
-79	ERROR_SC_TCOS_INITIALIZED	FATAL
-80	ERROR_SC_TCOS_PW1_INITIALIZED	FATAL
-81	ERROR_SC_TCOS_PW2_INITIALIZED	FATAL
-82	ERROR_SC_TCOS_SIGPW1_INITIALIZED	FATAL
-83	ERROR_SC_TCOS_SIGPW2_INITIALIZED	FATAL
-84	ERROR_SC_UNLOCK_PW1	FATAL
-85	ERROR_SC_UNLOCK_PW2	FATAL
-86	ERROR_SC_UNLOCK_SIGPW1	FATAL
-87	ERROR_SC_UNLOCK_SIGPW2	FATAL
-90	ERROR_TS_BUILD_REQUEST	FATAL
-91	ERROR_TS_GET_RESPONSE	FATAL
-92	ERROR_TS_GET_TIMESTAMP	FATAL
-93	ERROR_TS_TIMESTAMP_TO_LONG	FATAL
-94	ERROR_TS_NO_RSA_KEY	FATAL
-95	ERROR_TS_WRONG_PARAM	FATAL
-96	ERROR_CADES_LEVEL_NOT_SUPPORTED	FATAL
-113	Keine Signatur in der Datei vorhanden.	FATAL
-114	Die PKCS#7-Struktur ist fehlerhaft oder nicht vorhanden.	FATAL
-115	Die PKCS#7-Struktur ist fehlerhaft oder nicht vorhanden.	FATAL
-117	Die PKCS#1-Struktur ist fehlerhaft oder nicht vorhanden.	FATAL
-118	Das Zertifikat einer PKCS#1-Signatur ist fehlerhaft oder nicht vorhanden.	FATAL
-119	ERR_WRONG_PKCS7_SIGNATURE	FATAL
-120	ERR_WRONG_TSR_CONTENT	FATAL
-200	Das Verschlüsseln schlug fehl, da das Zertifikat ungültig ist.	FATAL
-201	Das Verschlüsseln schlug fehl, da die Nachricht ungültig ist.	FATAL
-202	Das Verschlüsseln schlug fehl, da die erzeugte Nachricht ungültig ist.	FATAL
-203	Das Verschlüsseln des Dokumentes schlug fehl.	FATAL
-204	Das Entschlüsseln schlug fehl, da das Zertifikat ungültig oder nicht vorhanden ist.	FATAL
-205	Das Entschlüsseln schlug fehl. Die verschlüsselte Nachricht konnte nicht verstanden werden.	FATAL
-206	Das Entschlüsseln schlug fehl. Das übergebene Dokument enthielt keine verschlüsselte Nachricht.	FATAL

-207	Das Entschlüsseln des Dokumentes schlug fehl.	FATAL
2164260866	ERROR_CAN_NOT_LOAD_SIGNATURE_FILE	FATAL
2164260868	ERROR_CAN_NOT_LOAD_TSR_FILE	FATAL
2164260872	ERROR_CAN_NOT_LOAD_DOC_FILE	FATAL
2147483649	ERROR_INVALID_SIGNATURE	FATAL
2147483650	ERROR_CERT	FATAL
2147483652	ERROR_CRL	FATAL
2147483656	ERROR_TRUST	FATAL
2147483664	ERROR_SERVER	FATAL
2147483680	ERROR_PERSON	FATAL
2147483712	ERROR_TIME_CERT	FATAL
2147483776	ERROR_CRL_ENTER	FATAL
2147483904	ERROR_CRL_TIME	FATAL
2147484160	ERROR_OCSP_COMM_ERROR	FATAL
2147484672	ERROR_OCSP_WRONG_RESPONSE	FATAL
2147485696	ERROR_OCSP_UNKNOWN	FATAL
2147487744	ERROR_SIGNOTCHECKED	FATAL
2147491840	ERROR_WRONG_CERT_SIGNATURE	FATAL
2147500032	ERROR_SIGN_NOT_INTIME	FATAL
2147516416	ERROR_SIGN_NOT_IN_CA_TIME	FATAL
2147418112	CA-Zertifikat nicht im Speicher gefunden!	FATAL
2147614720	ERROR_CRL_NOT_MATCH_CERT	FATAL
2147745792	WARNING_SIGN_OK_CERT_REV	FATAL
2148007936	Die OCSP-URl wurde nicht gefunden.	FATAL
2148532224	ERROR_TIMESTAMP	FATAL
2149580800	ERROR_TIMESTAMP_DOC	FATAL
2151677952	WARRNING_DOC_NOT_COVERED	FATAL
1073741825	ERROR_DEMAIL_UNSOPPORTED_VERSION	FATAL
1073741826	ERROR_DEMAIL_UNSOPPORTED_HASH_ALGORITHM	FATAL
1073741828	ERROR_DEMAIL_INVALID_V_TAG	FATAL
1073741832	ERROR_DEMAIL_INVALID_C_TAG	FATAL
1073741840	ERROR_DEMAIL_INVALID_H_TAG	FATAL
1073741856	ERROR_DEMAIL_INVALID_BODY_HASH	FATAL
1073741888	ERROR_DEMAIL_INVALID_HEADER_HASH	FATAL
1073741952	ERROR_DEMAIL_VALIDITY_HEADER_TOKENS	FATAL
1073742080	ERROR_DEMAIL_INVALID_LINEBREAKS	FATAL
1073742336	ERROR_DEMAIL_MUST_BE_SIGNED	FATAL
1073742848	ERROR_CAN_NOT_OPEN_DEMAIL_FILE	FATAL
1073743872	ERROR_DEMAIL_INVALID_HEADERS	FATAL
1073745920	ERROR_DEMAIL_INVALID_HEADER_SIGNATURE	FATAL
1073750016	ERROR_DEMAIL_NO_DATA	FATAL
1073758208	ERROR_DEMAIL_INVALID_SIGN	FATAL
1073774592	ERROR_DEMAIL_INVALID_CERT	FATAL
-256	MSSL_NO_DATA_PRESENT	FATAL
-257	MSSL_BUFFER_TO_SMALL	FATAL
-258	MSSL_NO_ACTIVE_PDF_DOC	FATAL
-259	MSSL_ERROR_OPENING_FILE	FATAL
-260	MSSL_ERROR_READING_FILE	FATAL
-261	MSSL_NO_FILE_NAME	FATAL
-262	MSSL_NO_DESTINATION_FIELD	FATAL
-263	MSSL_NO_FIELD_VALUE	FATAL
-264	MSSL_ERROR_ON_INTERNET_OPEN	FATAL
-265	MSSL_ERROR_ON_INTERNET_CONNECT	FATAL
-272	MSSL_ERROR_ON_OPEN_REQUEST	FATAL
-273	MSSL_ERROR_URL_CRACK	FATAL
-274	MSSL_ERROR_WRONG_PROTOCOL	FATAL
-275	MSSL_ERROR_NO_CERT_SELECTED	FATAL
-276	MSSL_ERROR_CLIENT_AUTH	FATAL
-277	MSSL_ERROR_INTERNET_CLOSE	FATAL
-1001	Die PDF-Datei konnte nicht gelesen werden.	FATAL
-1002	DasI nhaltsverzeichnis des PDF-Dokumentes konnte nicht gelesen werden	FATAL

-1003	Die Position des PDF-Trailers konnte nicht ermittelt werden.	FATAL
-1004	Beim Lesen eines PDF-Datenfeldes trat ein Fehler auf.	FATAL
-1007	Die Größe des Dokuments verhindert eine Verarbeitung.	FATAL
-1008	Die Eingabedaten sind ungültig.	FATAL
-1009	Der Stream-Start wurde im META-Objekt nicht gefunden.	FATAL
-1012	Die Eingabedatei konnte nicht geöffnet werden.	FATAL
-1013	ERROR_PDF_MAXSIZE	FATAL
-1014	ERROR_PDF_MEMORY_ALLOCATION	FATAL
-1016	Das Auslesen eines PDF-Feldwertes schlug fehl.	FATAL
-1018	Trailer des PDF-Dokumentes konnte nicht gelesen werden.	FATAL
-1021	Das Dokument ist verschlüsselt und kann daher nicht signiert werden.	FATAL
-1022	Die sichtbare Signatur konnte nicht innerhalb der Seitenränder positioniert werden.	FATAL
-1023	Es konnte keine Instanz des signierten PDF-Dokumentes angelegt werden.	FATAL
-1025	Es wurde kein signaturfähiger Inhalt gefunden.	FATAL
-1026	Das Hinzufügen einer PDF-Anlage schlug fehl.	FATAL
-1027	Ein Objekt zur sichtbaren Unterschrifsdarstellung konnte nicht in das PDF-Dokument eingefügt werden.	FATAL
-1028	Die übergebene Grafikdatei konnte nicht geöffnet oder gelesen werden.	FATAL
-1029	Die übergebene Datei ist kein PDF-Dokument	FATAL
-1030	Das Pages-Objekt enthält keinen Count-Eintrag.	FATAL
-1031	Unbekanntes Annotate-Array gefunden.	FATAL
-1032	Das PDF ist linearisiert.	FATAL
-1033	Im PDF wurden keine Seiten gefunden.	ERROR
-1050	Die Seitengröße des Dokumentes konnte nicht ermittelt werden.	FATAL
-1051	Die Begründung ist zu lang.	FATAL
-1052	Der Ort ist zu lang.	FATAL
-1035	Das angegebene Hintergrundbild der Signatur ist nicht im JPEG-Format	FATAL
-1038	Das PDF-Dokument konnte nicht angelegt oder geschrieben werden.	FATAL
-1040	Ein Datumsfeld hat ein inkorrektes Format.	FATAL
-1081	Das Dokument konnte nicht gelesen werden.	FATAL
-1171	Das anzufügende Dokument konnte nicht geöffnet werden.	FATAL
-1172	Ein Datenblock konnte dem PDF-Dokument nicht hinzugefügt werden.	FATAL
-1173	Anhang konnte dem PDF-Dokument nicht hinzugefügt werden. Nicht unterstützter MIME-Typ.	FATAL
-1801	Die Bestimmung der Signaturposition war nicht erfolgreich.	FATAL
-1200	Das Durchsuchen des PDF-Dokumentes schlug fehl.	FATAL
-1201	Ein unbekannter Schrifttyp wurde gefunden.	FATAL
-1300	Der neue Name für die PDF-Collection ist leer.	FATAL
-1301	Die Liste der PDF-Collection ist leer.	FATAL
-1302	In der PDF-Collection-Liste steht ein leerer Dateiname.	FATAL
-1303	ERROR_PDFCOLLECTION_LIST_FTYPE_PROBLEM	FATAL
-1304	PDF-Collection-Liste iste keine aktive Seite definiert.	FATAL
-1305	Die PDF-Collection hat eine Datei nicht gefunden.	FATAL
-1306	Die PDF-Collection hat keine Titelseite.	FATAL
-1307	ERROR_COVERSHEETISLINEARIZED	FATAL
-1308	ERROR_COVERSHEETMORE14	FATAL
-10001	ERROR_TIFF_UNKNOWN_ERROR	FATAL
-10002	ERROR_TIFF_PRECEDING_ERROR	FATAL
-10100	ERROR_TIFF_STREAM_IS_NULL	FATAL
-10101	ERROR_TIFF_STREAM_IS_NOT_OPEN	FATAL
-10102	ERROR_TIFF_PROVIDED_ARRAY_IS_TOO_SMALL	FATAL
-10200	ERROR_TIFF_NO_VALID_TIFF	FATAL
-10201	ERROR_TIFF_NO_VALID_TIFF_HEADER	FATAL
-10202	ERROR_TIFF_DESCRIPTION_TAGS_INVALID	FATAL
-10300	TIFF-Signatur wurde nicht gefunden.	FATAL
-10301	ERROR_TIFF_INVALID_SIGNATURE_INDEX	FATAL
-10400	Datei wurde nicht gefunden.	FATAL
-10400	ERROR_TIFF_ILLEGAL_ARGUMENT	FATAL

7.3 SQL-Datenbank Protokollierung

Damit auftretende Eregnisse in einer Datenbank gespeichert werden können, müssen folgende Voraussetzungen gegeben sein:

- SQL-Datenbank mit entsprechender Tabelle
- Zugriffsrechte
- Korrekte Zugangsdaten für den AV DCE
- ODBC-Zugang

Auf dem SQL-Server muss eine Datenbank mit folgenden Tabellen vorhanden sein:

- events
- module
- severity

Weiterhin sollte es dort eine Sicht

- showevents

geben.

Für die Erstellung der Tabellen, der Schlüssel und der Sicht gibt es SQL-Scripte.

7.3.1 Script zur Erstellung der Tabellen und Schlüssel (SQL-Logging)

Folgendes Script muss auf einem Microsoft SQL-Server gestartet werden, um die entsprechenden Tabellen für ein mögliches Logging zu erzeugen.

```
/****** DB Skript für MS SQL Server ******/
Use [AV DCE];

/*************************/
/****** DROP TABLES ******/
/*************************/

/****** Object:  Table [dbo].[module] ******/
IF  EXISTS (SELECT * FROM sys.foreign_keys WHERE object_id =
OBJECT_ID(N'[dbo].[fk_events_module]') AND parent_object_id = OBJECT_ID(N'[dbo].[events]'))
ALTER TABLE [dbo].[events] DROP CONSTRAINT [fk_events_module]
GO
```

```
IF  EXISTS (SELECT * FROM sys.foreign_keys WHERE object_id =
OBJECT_ID(N'[dbo].[fk_events_severity]') AND parent_object_id = OBJECT_ID(N'[dbo].[events]'))
ALTER TABLE [dbo].[events] DROP CONSTRAINT [fk_events_severity]
GO

IF  EXISTS (SELECT * FROM sys.objects WHERE object_id = OBJECT_ID(N'[dbo].[module]') AND type in
(N'U'))
DROP TABLE [dbo].[module]
GO

/****** Object:  Table [dbo].[severity] ******/
IF  EXISTS (SELECT * FROM sys.objects WHERE object_id = OBJECT_ID(N'[dbo].[severity]') AND type
in (N'U'))
DROP TABLE [dbo].[severity]
GO

/****** Object:  Table [dbo].[events] ******/
IF  EXISTS (SELECT * FROM sys.objects WHERE object_id = OBJECT_ID(N'[dbo].[events]') AND type in
(N'U'))
DROP TABLE [dbo].[events]
GO

/****** Object:  View [dbo].[showevents] ******/
IF  EXISTS (SELECT * FROM sys.views WHERE object_id = OBJECT_ID(N'[dbo].[showevents]'))
DROP VIEW [dbo].[showevents]
GO


/***************************/
/****** CREATE TABLES ******/
/***************************/

/****** Object:  Table [dbo].[events] ******/
CREATE TABLE [dbo].[events](
	[id] [int] IDENTITY(1,1) NOT NULL,
	[tstamp] [varchar](30) NOT NULL,
	[severityid] [int] NULL,
	[moduleid] [int] NULL,
	[msg] [varchar](255) NULL,
	[file] [varchar](255) NULL,
 CONSTRAINT [PK_Events] PRIMARY KEY CLUSTERED
(
	[id] ASC
)WITH (PAD_INDEX  = OFF, STATISTICS_NORECOMPUTE  = OFF, IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS  =
ON, ALLOW_PAGE_LOCKS  = ON) ON [PRIMARY]
) ON [PRIMARY]
GO

/****** Object:  Table [dbo].[module] ******/
CREATE TABLE [dbo].[module](
	[id] [int] NOT NULL,
	[description] [varchar](255) NOT NULL,
 CONSTRAINT [pk_module] PRIMARY KEY CLUSTERED
(
	[id] ASC
)WITH (PAD_INDEX  = OFF, STATISTICS_NORECOMPUTE  = OFF, IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS  =
ON, ALLOW_PAGE_LOCKS  = ON) ON [PRIMARY]
) ON [PRIMARY]
GO

/****** Object:  Table [dbo].[severity] ******/
```

```
CREATE TABLE [dbo].[severity](
	[id] [int] NOT NULL,
	[description] [varchar](255) NOT NULL,
 CONSTRAINT [pk_severity] PRIMARY KEY CLUSTERED
(
	[id] ASC
)WITH (PAD_INDEX  = OFF, STATISTICS_NORECOMPUTE  = OFF, IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS  =
ON, ALLOW_PAGE_LOCKS  = ON) ON [PRIMARY]
) ON [PRIMARY]
GO


/****** FK´s ******/
ALTER TABLE [dbo].[events]  WITH CHECK ADD  CONSTRAINT [fk_events_module] FOREIGN KEY([moduleid])
REFERENCES [dbo].[module] ([id])
GO

ALTER TABLE [dbo].[events] CHECK CONSTRAINT [fk_events_module]
GO

ALTER TABLE [dbo].[events]  WITH CHECK ADD  CONSTRAINT [fk_events_severity] FOREIGN
KEY([severityid])
REFERENCES [dbo].[severity] ([id])
GO

ALTER TABLE [dbo].[events] CHECK CONSTRAINT [fk_events_severity]
GO

/*************************************/
/****** Erstellung Default-Inhalte *****/
/*************************************/
INSERT INTO severity (id, description) VALUES(0, 'Success');
INSERT INTO severity (id, description) VALUES(1, 'Info');
INSERT INTO severity (id, description) VALUES(2, 'Warning');
INSERT INTO severity (id, description) VALUES(3, 'Failure');
INSERT INTO severity (id, description) VALUES(4, 'Fatal error');

INSERT INTO module (id, description) VALUES(1, 'Signature engine');
INSERT INTO module (id, description) VALUES(2, 'Signature session monitoring');
INSERT INTO module (id, description) VALUES(3, 'Verification engine');
INSERT INTO module (id, description) VALUES(4, 'Configuration store');
INSERT INTO module (id, description) VALUES(5, 'Document preprocessing');
INSERT INTO module (id, description) VALUES(6, 'Document postprocessing');
INSERT INTO module (id, description) VALUES(7, 'Image conversion module');
INSERT INTO module (id, description) VALUES(8, 'Core Application');
INSERT INTO module (id, description) VALUES(9, 'Copy Protection module');
INSERT INTO module (id, description) VALUES(10, 'SOAP Connector');
INSERT INTO module (id, description) VALUES(11, 'Kofax Textplus Connector');
INSERT INTO module (id, description) VALUES(12, 'SMTP Connector');
INSERT INTO module (id, description) VALUES(13, 'MessageQueue Connector');
INSERT INTO module (id, description) VALUES(14, 'Remote Connector');
INSERT INTO module (id, description) VALUES(15, 'Timestamp engine');
INSERT INTO module (id, description) VALUES(16, 'Timestamp session');
INSERT INTO module (id, description) VALUES(17, 'Kodak engine');
INSERT INTO module (id, description) VALUES(18, 'Verification session');
INSERT INTO module (id, description) VALUES(19, 'Filestore engine');
```

7.3.2 Script zur Erstellung der Sicht „showevents“

Für eine gut lesbare Anzeige der Logging-Events auf dem Microsoft SQl-Serv kann mit nachfolgendem Script eine Sicht angelegt werden.

```
CREATE VIEW [dbo].[showevents]
AS
SELECT     dbo.events.id, dbo.events.tstamp, dbo.events.severityid, dbo.events.moduleid,
dbo.events.msg, dbo.events.[file], dbo.module.description AS moduledescription,
                      dbo.severity.description AS severitydescription
FROM         dbo.events INNER JOIN
                      dbo.module ON dbo.events.moduleid = dbo.module.id INNER JOIN
                      dbo.severity ON dbo.events.severityid = dbo.severity.id

GO
```

7.3.3 Einrichtung Zugang

Zur Einrichtung des Zugangs zum SQL-Server muss eine ODBC-Quelle eingerichtet werden:

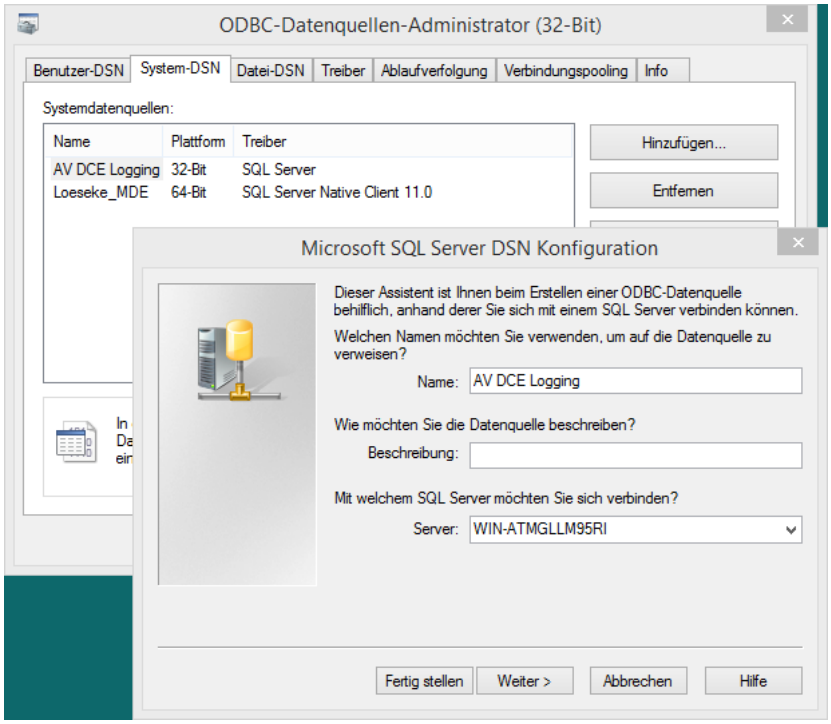


Abbildung 7-1 Einrichtung ODBC-Datenquelle

Die Anmeldedaten für den Benutzer auf dem SQL-Server müssen in der ODBC-Quelle eingetragen werden:

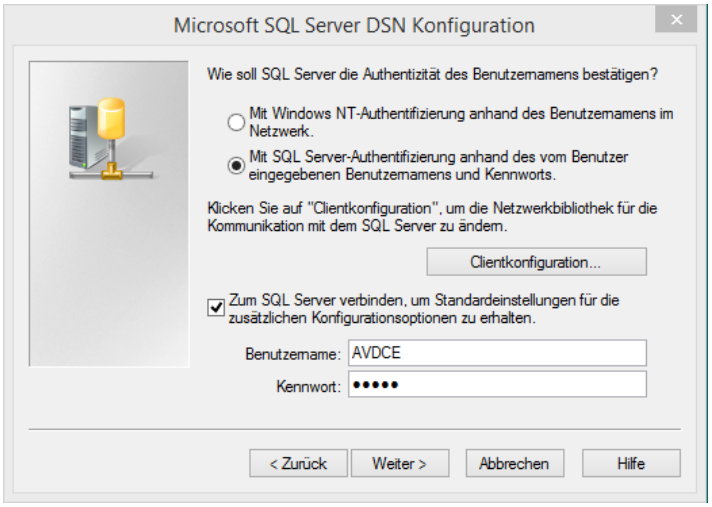


Abbildung 7-2 Einrichtung ODBC-Daten

Danach muss dem AV DCE ebenfalls die Anmeldedaten und der ODBC-Quellenname mitgeteilt werden.

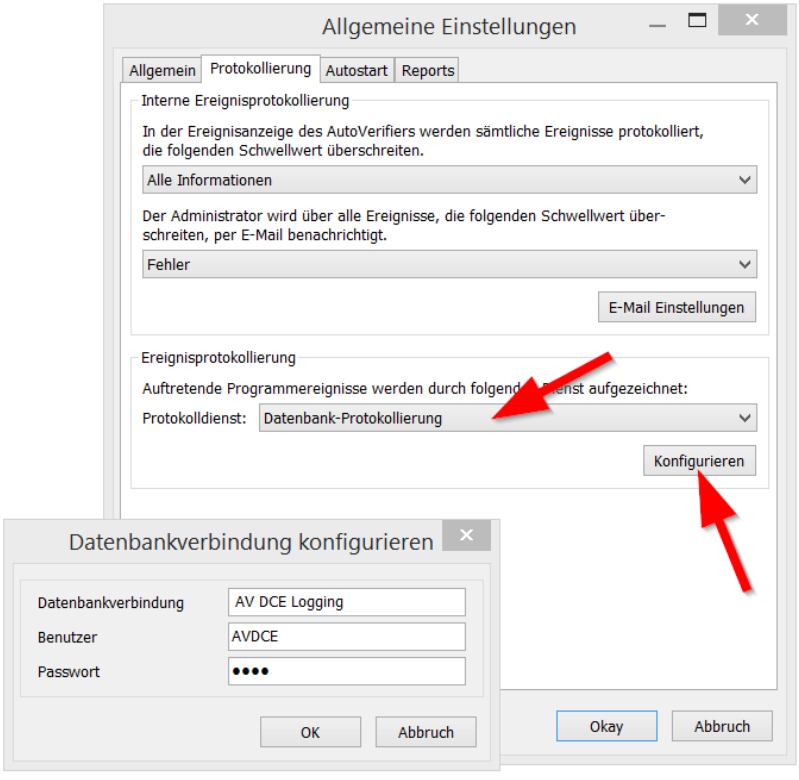


Abbildung 7-3 Konfiguration ODBC im AV DCE

Nach dem erneuten Starten des AV DCE erfolgt die Ausgabe der Log-Meldungen in die Datenbank.

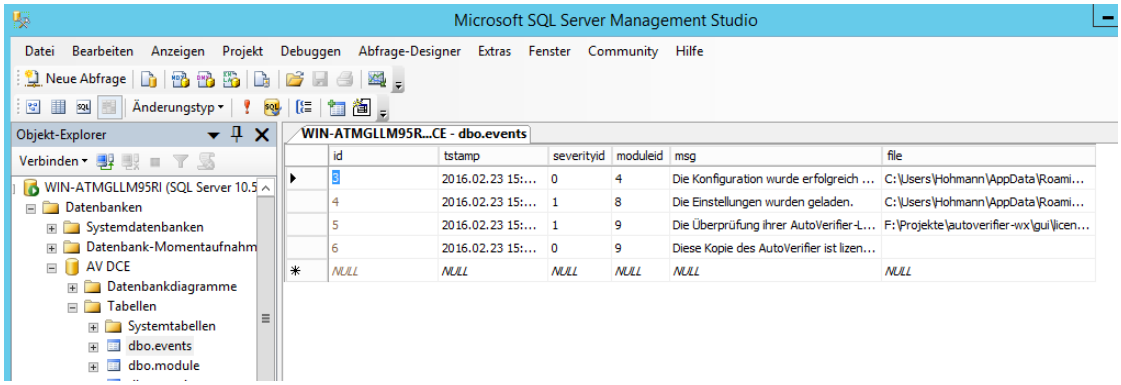


Abbildung 7-4 Beispielanzeige Tabelle 'events' im SQL-Server

7.4 Beispiel Config.xml

```
<?xml version="1.0" encoding="ISO-8859-1" standalone="yes"?>
<configuration product="AutoVerifier" version="1.1">
    <gui>
        <showlogging>false</showlogging>
        <showshortfilenames>false</showshortfilenames>
        <guisvcshowname>autoverifierDCE</guisvcshowname>
        <modus>stdalone</modus>
    </gui>
    <core>
        <operationmode>FILESTORE</operationmode>
        <language>GERMAN</language>
        <threadcount>5</threadcount>
        <logging>
            <threshold>
                <eventview>ALL</eventview>
                <email>FAILURE</email>
            </threshold>
            <emailsettings>
                <sendername/>
                <senderaddr/>
                <recipient/>
                <replyto/>
                <authrequired>true</authrequired>
                <server/>
                <user/>
                <passwd/>
                <digest>true</digest>
                <digestmode>DAILY</digestmode>
                <digestsize>10</digestsize>
            </emailsettings>
            <logger>
                <type>ROLLINGFILE</type>
                <location>D:\Users\hohmann\AppData\Roaming\Mentana\AutoVerifier DCE\log</location>
            </logger>
        </logging>
        <remoteconnector>
            <activated>false</activated>
            <port>7880</port>
            <threshold>ALL</threshold>
            <showevents>true</showevents>
            <users>
                <user-account>
                    <name>administrator</name>
                    <password>start</password>
                </user-account>
            </users>
        </remoteconnector>
        <session>
            <autostart>
                <active>false</active>
            </autostart>
        </session>
        <ssl>
            <usage>false</usage>
            <capath/>
            <cafile/>
        </ssl>
        <verification>
            <checkmode>
                <integrity>true</integrity>
                <name>false</name>
                <chain>true</chain>
                <time>true</time>
                <rev>true</rev>
```

```
</checkmode>
<revocation>
    <csp>true</csp>
    <x509>false</x509>
    <file>false</file>
    <ocsp>false</ocsp>
    <ldap>false</ldap>
    <http>false</http>
    <url/>
</revocation>
<onlinetimeout>15000</onlinetimeout>
<ocspcaching>
    <activated>false</activated>
    <validity>300</validity>
</ocspcaching>
<lmntproxy>
    <activated>false</activated>
    <address/>
    <port>8080</port>
</lmntproxy>
<ocspresponder>
    <responder>
        <issuer>TeleSec PKS SigG CA 1:PN</issuer>
        <serial/>
        <url>http://pks.telesec.de/ocspr</url>
        <activated>true</activated>
    </responder>
    <responder>
        <issuer>TeleSec PKS SigG CA 13:PN</issuer>
        <serial/>
        <url>http://pks.telesec.de/ocspr</url>
        <activated>true</activated>
    </responder>
    <responder>
        <issuer>TeleSec PKS SigG CA 17 1:PN</issuer>
        <serial/>
        <url>http://pks.telesec.de/ocspr</url>
        <activated>true</activated>
    </responder>
    <responder>
        <issuer>a-sign-corporate-light-03</issuer>
        <serial>01AAED</serial>
        <url>http://ocsp.a-trust.at/ocsp</url>
        <activated>true</activated>
    </responder>
</ocspresponder>
<filetypemap>
    <filetype>
        <description>PDF-Documents</description>
        <extension>PDF</extension>
        <action>PDF_DOCUMENT</action>
        <activated>true</activated>
    </filetype>
    <filetype>
        <description>Enveloped S/MIME</description>
        <extension>P7M</extension>
        <action>SMIME_ENVELOPED_SIGNATURE</action>
        <activated>true</activated>
    </filetype>
    <filetype>
        <description>Enveloped S/MIME</description>
        <extension>PKCS7M</extension>
        <action>SMIME_ENVELOPED_SIGNATURE</action>
        <activated>true</activated>
    </filetype>
    <filetype>
        <description>Signed TIFF-Documents</description>
        <extension>TIF</extension>
        <action>TIFF_DOCUMENT</action>
        <activated>true</activated>
```

```
            </filetype>
            <filetype>
                <description>Signed TIFF-Documents</description>
                <extension>TIFF</extension>
                <action>TIFF_DOCUMENT</action>
                <activated>true</activated>
            </filetype>
            <filetype>
                <description>Detached S/MIME</description>
                <extension>P7S</extension>
                <action>SMIME_DETACHED_SIGNATURE</action>
                <activated>true</activated>
            </filetype>
            <filetype>
                <description>Detached S/MIME</description>
                <extension>PKCS7</extension>
                <action>SMIME_DETACHED_SIGNATURE</action>
                <activated>true</activated>
            </filetype>
            <filetype>
                <description>Timestamp Response</description>
                <extension>TSR</extension>
                <action>SMIME_DETACHED_SIGNATURE</action>
                <activated>true</activated>
            </filetype>
            <filetype>
                <description>De-Mail (.eml)</description>
                <extension>EML</extension>
                <action>DEMAIL_DOCUMENT</action>
                <activated>true</activated>
            </filetype>
            <filetype>
                <description>De-Mail (.demail)</description>
                <extension>DEMAIL</extension>
                <action>DEMAIL_DOCUMENT</action>
                <activated>true</activated>
            </filetype>
            <filetype>
                <description>Mailbox (.mbox)</description>
                <extension>MBOX</extension>
                <action>MAILBOX_DOCUMENT</action>
                <activated>true</activated>
            </filetype>
        </filetypemap>
        <mode>CHAIN</mode>
    </verification>
    <report>
        <xml>
            <enabled>true</enabled>
            <prefix/>
            <suffix/>
            <stylesheet>http://www.mentana.de/verification/xsl/MentanaV3Result.xslt</stylesheet>
            <skipextension>false</skipextension>
        </xml>
        <pdf>
            <enabled>true</enabled>
            <prefix/>
            <suffix>_report</suffix>
            <stylesheet>E:\Projekte\autoverifier-wx\gui\stylesheet\mentana.xsl</stylesheet>
            <fophostname>localhost</fophostname>
            <fopport>1111</fopport>
            <skipextension>true</skipextension>
        </pdf>
        <collection>
            <enabled>false</enabled>
            <prefix/>
            <suffix>_package</suffix>
            <coversheet/>
            <skipextension>true</skipextension>
            <deletereport>false</deletereport>
```

```
                <showcoverpage>true</showcoverpage>
            </collection>
            <timestamp>
                <enabled>false</enabled>
                <serverurl>http://tsa.mentana-net.de/tsa/service</serverurl>
                <hashalgo>SHA-256</hashalgo>
            </timestamp>
        </report>
    </core>
    <filestoreengine>
        <folders>
            <in>D:\Users\hohmann\AppData\Roaming\Mentana\AutoVerifier DCE\in</in>
            <out>D:\Users\hohmann\AppData\Roaming\Mentana\AutoVerifier DCE\out</out>
            <backup>D:\Users\hohmann\AppData\Roaming\Mentana\AutoVerifier DCE\backup</backup>
            <report>D:\Users\hohmann\AppData\Roaming\Mentana\AutoVerifier DCE\report</report>
            <error>D:\Users\hohmann\AppData\Roaming\Mentana\AutoVerifier DCE\error</error>
        </folders>
        <behaviour>
            <sigfileextensions>pkcs7,p7s</sigfileextensions>
            <createbackup>true</createbackup>
            <scansubfolders>false</scansubfolders>
            <writeresult>false</writeresult>
        </behaviour>
        <priority>2</priority>
        <conflicthandling>
            <stoponfileerror>false</stoponfileerror>
            <conflictaction>OVERWRITE_FILE</conflictaction>
            <conflictskip>
                <createskipfile>false</createskipfile>
                <skipfileextension>skip</skipfileextension>
            </conflictskip>
            <conflictrename>
                <numbering>PAST_PREFIX</numbering>
                <prefix/>
                <suffix/>
            </conflictrename>
        </conflicthandling>
    </filestoreengine>
    <soapengine>
        <engine-id>1</engine-id>
        <queuedatabase>
            <dsn>avsoap</dsn>
            <user>AV_User</user>
            <password>start</password>
        </queuedatabase>
    </soapengine>
    <smtpengine>
        <engine-id>1</engine-id>
        <queuedatabase>
            <dsn>avsoap</dsn>
            <user>AV_User</user>
            <password>start</password>
        </queuedatabase>
    </smtpengine>
</configuration>
```

7.5 AVPDF-Service

Der AVPDFService soll als Dienst aus übergebenen Daten eine PDF-Datei erstellen. Es wird eine Datendatei, sowie ein Stylesheet via Socket übertragen, damit der AVPDFService korrekt arbeiten kann.
Intern verwendet der AVPDFService die Bibliotheken Apache FOP und Apache XML Graphics. Die Ansteuerung erfolgt aus dem AV DCE heraus.

Weitere Einstellungen am Service brauchen nicht vorgenommen zu werden.

7.6 SOAP-Connector

Anachfolgend ein Beispiel-Schema für die Datenbank-Einstellungen (Postgress) für den SOAP-Connector.

Der AV DCE greift auf folgende Felder zu:

Tabelle	Feld	Zugriffsart
Tasks	Id	R/W
Tasks	statusid	R/W
Tasks	processresult	W
Tasks	reporttypeid	W
Tasks	localfilename	R
Tasks	filename	R
Tasks	filetypeid	R
Tasks	engineID	R
Engines	Statusid	R/W
Engines	Id	R
Engines	Name	R
Engines	Spooldir	R

```
/*
        AutoverifierSOAP-Connector database SCHEMA FOR POSTGRES 8
*/


DROP TABLE IF EXISTS enginestatus ;
DROP TABLE IF EXISTS engines ;
DROP TABLE IF EXISTS tasks  ;
DROP TABLE IF EXISTS taskstatus ;
DROP TABLE IF EXISTS filetype ;
DROP SEQUENCE IF EXISTS sq_tasks ;
DROP SEQUENCE IF EXISTS sq_engines ;


CREATE SEQUENCE sq_tasks ;
CREATE SEQUENCE sq_engines ;


CREATE TABLE engines
(
        id              INTEGER         NOT NULL,
        NAME            VARCHAR(128)    NOT NULL,
        spooldir        VARCHAR(256)    NOT NULL,
```

```
        faileddir       VARCHAR(256)    NOT NULL,
        statusid        INTEGER         NOT NULL,
        PRIMARY KEY(id)
) ;


CREATE TABLE tasks
(
      id              INTEGER        NOT NULL,
      token           VARCHAR(64)    NOT NULL,
      engineid        INTEGER        NOT NULL,
      filename        VARCHAR(512)   NOT NULL,
      localfilename   VARCHAR(512)   NOT NULL,
      rectime         TIME           NOT NULL,
      processed       TIME,
      processresult   INT            NULL,
      filetypeid      INT            NOT NULL,
      statusid        INTEGER        NOT NULL,
      reporttypeid    INT            NULL,
      remotemsg       VARCHAR(1024),
      reason          VARCHAR(512)   NULL,
      locatio         VARCHAR(512)   NULL,
      signfilename    VARCHAR(512)   NULL,
      customerId      VARCHAR(512)   NULL,
      PRIMARY KEY (id)
);


CREATE TABLE enginestatus
(
        id              INTEGER         NOT NULL,
        descr           VARCHAR(50)     NOT NULL,
        PRIMARY KEY(id)
) ;


CREATE TABLE taskstatus
(
        id              INTEGER         NOT NULL,
        descr           VARCHAR(50)     NOT NULL,
        PRIMARY KEY(id)
) ;

CREATE TABLE filetype
(
        id              INTEGER         NOT NULL,
        NAME            VARCHAR(50)     NOT NULL,
        ext_sig         BOOL,
        PRIMARY KEY(id)
) ;


INSERT INTO enginestatus(id, descr) VALUES(1, 'offline') ;
INSERT INTO enginestatus(id, descr) VALUES(2, 'running') ;
INSERT INTO enginestatus(id, descr) VALUES(3, 'paused') ;


INSERT INTO engines(id, NAME, spooldir, faileddir, statusid)
VALUES(1, 'Autoverifier SOAP Engine', 'c:\\server\\autoverifier\\spool',
'c:\\server\\autoverifier\\spool\\failed', 1) ;


INSERT INTO taskstatus(id, descr) VALUES(1, 'uploading') ;
INSERT INTO taskstatus(id, descr) VALUES(2, 'waiting for processing') ;
INSERT INTO taskstatus(id, descr) VALUES(3, 'waiting for preprocessing') ;
INSERT INTO taskstatus(id, descr) VALUES(4, 'processing') ;
INSERT INTO taskstatus(id, descr) VALUES(5, 'waiting for postprocessing') ;
INSERT INTO taskstatus(id, descr) VALUES(6, 'finished') ;
INSERT INTO taskstatus(id, descr) VALUES(7, 'failed') ;
INSERT INTO taskstatus(id, descr) VALUES(8, 'cancelled') ;
```

```
INSERT INTO taskstatus(id, descr) VALUES(9, 'moved to another queue') ;
INSERT INTO taskstatus(id, descr) VALUES(10, 'subtask finished') ;
INSERT INTO taskstatus(id, descr) VALUES(11, 'task status undetermined') ;

INSERT INTO filetype(id, NAME, ext_sig) VALUES(1, 'PDF document',               FALSE) ;
INSERT INTO filetype(id, NAME, ext_sig) VALUES(2, 'JPEG image',                 TRUE) ;
INSERT INTO filetype(id, NAME, ext_sig) VALUES(3, 'TIFF image',                 TRUE) ;
INSERT INTO filetype(id, NAME, ext_sig) VALUES(4, 'S/MIME signature',   TRUE) ;
INSERT INTO filetype(id, NAME, ext_sig) VALUES(5, 'Binary data',                TRUE) ;
```

7.7 weiterführende Infos

https://de.wikipedia.org/wiki/Online_Certificate_Status_Protocol

https://www.informatik.tu-darmstadt.de/BS/Lehre/Sem98_99/T11/

https://www.tuhh.de/rzt/it-sicherheit/tuhh-dfnpki/zertifikate.html

https://de.wikipedia.org/wiki/NTLM

7.8 Abbildungsverzeichnis

Abbildung 3-1 Auswahl des Installationsortes 8
Abbildung 3-2 AutoVerifier DCE in der Windows-Dienstverwaltung 9
Abbildung 3-3 Lizenzprüfung 9
Abbildung 3-4 Allgemeine Lizenzanzeige 10
Abbildung 4-42 Eigenschaften des AV DCE-Dienstes 12
Abbildung 4-43 Konsole im Admin-Modus 12
Abbildung 4-44 Der installierte AVDCE im Dienstmanager 14
Abbildung 4-1 GUI im Dienst-Modus mit Service-Logging 14
Abbildung 4-2 Symbolleiste Dienst-Modus (zuwenig Rechte) 15
Abbildung 4-4 Allgemeine Einstellungen 16
Abbildung 4-5 Schema Dateibasierte Schnittstelle 17
Abbildung 4-6 Schema SOAP-Schnittstelle 17
Abbildung 4-7 Schema SMTP-Schnittstelle 18
Abbildung 4-8 Protokollierung 19
Abbildung 4-9 Konfiguration E-Mail-Server 20
Abbildung 4-10 Log-Verzeichnis auswählen (Textdatei-Protokollierung) 21
Abbildung 4-11 Parameter für die Datenbank-Protokollierung 22
Abbildung 4-12 Allgemeine Einstellung – Autostart 22
Abbildung 4-13 Report 23
Abbildung 4-14 Liste der Dienste mit markiertem AVPDFService 25
Abbildung 4-15 Erfolgreicher FOP-Check 25
Abbildung 4-16 Gestoppter FOP-Dienst beim Check 26
Abbildung 4-17 FOP-Dienst konnte via Socket nicht erreicht werden 26
Abbildung 4-18 Verifikationseigenschaften 29
Abbildung 4-19 SSL-Verifikationseinstellungen 32
Abbildung 4-20 NTLM-Einstellungen 33
Abbildung 4-21 Anzeige Zertifikat mit OCSP-Daten 34
Abbildung 4-22: OCSP-Responder 34
Abbildung 4-23 Eigenschaften OCSP-Responder 35
Abbildung 4-24 Einschaften OCSP-Responder Beispieldaten 35
Abbildung 4-25 Dialog zur Festlegung der Verzeichnisse 36
Abbildung 4-26 Konfliktbehandlung 37
Abbildung 4-27: Dialog zur Festlegung des Verhaltens beim Überspringen von Dateien 38
Abbildung 4-28: Dialog zum Festlegen des Verhaltens beim Umbenennen von Dateien 38
Abbildung 4-29: Dateierweiterungen 40
Abbildung 4-30 Dateitypen-Behandlung 40
Abbildung 4-32 Einrichten Verbindungsdatenbank 42
Abbildung 4-33 Betriebsmodus SOAP-Connector 43
Abbildung 4-34: Remoteconsole konfigurieren 44
Abbildung 4-35 Windows Sicherheitshinweis der Firewall 44

Abbildung 4-36 Kommandozeile mit gestartetem Telnet-Zugriff....45
Abbildung 4-37 Einloggen und Log-Meldung....46
Abbildung 4-38 Statistik....47
Abbildung 4-39 GUI-Einstellungen....47
Abbildung 4-40 AV DCE-Dienste Auflistung....48
Abbildung 4-41 Info-Fenster....49
Abbildung 5-1 AV DCE Gui....51
Abbildung 5-2 AutoVerifier DCE....52
Abbildung 5-3 Dienste-Anzeige mit Eigenschaften/ Anmeldedaten....60
Abbildung 6-1 Icon Anzeige Info-Fenster....62
Abbildung 6-2 Info-Fenster mit markierten Log-Informationen....62
Abbildung 6-3 Abschnitt in der Config.xml über Logging-Location....63
Abbildung 7-1 Einrichtung ODBC-Datenquelle....73
Abbildung 7-2 Einrichtung ODBC-Daten....74
Abbildung 7-3 Konfiguration ODBC im AV DCE....74
Abbildung 7-4 Beispielanzeige Tabelle 'events' im SQL-Server....75

7.9 Stichwortverzeichnis

Anwendungsmodi 52
Konfigurationsdatei 49
Lizenz-Datei 9
Logdateien 62
Schutzmechanismus 6