

AI WEBLAUNCHER

Installation und Betrieb



Version: 1.1.3
Projekt: AI WEBLAUNCHER
Datum: 1. April 2020

Dokumentinformation:

Erstellt von:	Administration Intelligence AG
E-Mail:	produktmanagement@ai-ag.de

Änderungshistorie:

Datum	Version	Änderung
20.02.2019	1.0	Initiale Erstellung

Inhaltsverzeichnis

0	Release Notes	4
1	Überblick	5
2	Installation	6
2.1	Installation mit grafischer Oberfläche	6
2.2	Installation ohne grafische Oberfläche	10
2.2.1	Fragen in der Kommandozeile beantworten	10
2.2.2	Konfiguration als Parameter übergeben	11
2.3	Starten von Anwendungen mittels AI WEBLAUNCHER	11
2.3.1	Mime-Type-Verknüpfung	11
2.3.2	Speicherort	11
2.3.2.1	Logausgaben	12
2.3.2.2	Neuen Download der Applikation erzwingen	12
2.3.3	Verwendete Version von AI WEBLAUNCHER auslesen	12
2.3.4	Besonderheiten unter Windows	12
3	Netzwerkstruktur und Sicherheit	14
3.1	Proxy-Dialog	14
3.2	Server-Authentisierung-Dialog	14
3.3	SSL-Dialog	15
3.4	Auslieferung von Proxy-, Server- und SSL-Einstellungen durch zentrale Verteilung	16

0 Release Notes

Die folgende Tabelle listet die Software-Änderungen in den einzelnen Versionen des **AI WEBLAUNCHER** auf.

Version	Release Notes
1.0.3	<ul style="list-style-type: none">• Initiale Freigabe
1.0.4	<ul style="list-style-type: none">• Neue Code-Signatur zur Vermeidung der Smartscreen Defender Warnmeldung bei der Installation• Erweiterung des Betriebshandbuchs
1.0.5	<ul style="list-style-type: none">• Erweiterung des Betriebshandbuchs
1.0.6	<ul style="list-style-type: none">• Fehlerbericht kann nun erzeugt werden, wenn der Anwendungsstart fehlschlägt• Wechsel von Verbindung mit Proxy auf eine direkte Verbindung funktioniert jetzt• Englische Sprache ist jetzt Standard, falls Sprache des Betriebssystems nicht unterstützt bzw. erkannt wird
1.1.0	<ul style="list-style-type: none">• Anwendungen können im DEBUG Modus gestartet werden• Validierung der Code-Signatur beim Start einer Anwendung
1.1.1	<ul style="list-style-type: none">• MacOS Notarisierung hinzugefügt• Serverauthentisierung wurde hinzugefügt• Zentrale Verteilung von SSL-Zertifikaten und Proxy- bzw. Server-Zugangsdaten• Vorherige Java Laufzeitumgebung wird nun bei einem Update korrekt gelöscht
1.1.2	<ul style="list-style-type: none">• Fehler bei Installation auf MacOS behoben• Backslashes im Benutzernamen von Proxy-Zugangsdaten nun verwendbar
1.1.3	<ul style="list-style-type: none">• Versionsüberprüfung bei Start der Applikation

1 Überblick

AI WEBLAUNCHER ist eine moderne und auf Open-Source-Komponenten aufbauende Lösung, um die Produkte der Administration Intelligence AG zukünftig starten zu können. **AI WEBLAUNCHER** ersetzt Oracles Java Web Start Technologie, die damit nicht mehr notwendig ist, um Desktop-Anwendungen der Administration Intelligence AG zu starten.

2 Installation

2.1 Installation mit grafischer Oberfläche

Beim Start der Installation mithilfe der Installationsdatei von **AI WEBLAUNCHER** kann eine Hinweismeldung des Smartscreen Defenders von Windows erscheinen. Wenn die **AI WEBLAUNCHER** Installationsdatei aus einer sicheren Quelle bezogen wurde, kann mit einem Klick auf „Weitere Informationen“ und „Trotzdem ausführen“ die Installation gestartet werden.

Bei einem Administratorenkonto wird man durch die Benutzerkontensteuerung aufgefordert das Installationsprogramm mit Administratorenrechten zu starten. Bei einem normalen Benutzerkonto kann **AI WEBLAUNCHER** nur in Verzeichnisse mit Schreibrechten installiert werden. Üblicherweise ist dies das Benutzerverzeichnis.



Abbildung 1: Startbildschirm der **AI WEBLAUNCHER** Installation

Im 2. Schritt der Installation von **AI WEBLAUNCHER** muss der Lizenzvereinbarung zugestimmt werden, um mit der Installation fortfahren zu können.



Abbildung 2: Lizenzvereinbarung der **AI WEBLAUNCHER** Installation

Im nächsten Schritt kann das Installationsverzeichnis von **AI WEBLAUNCHER** ausgewählt werden.

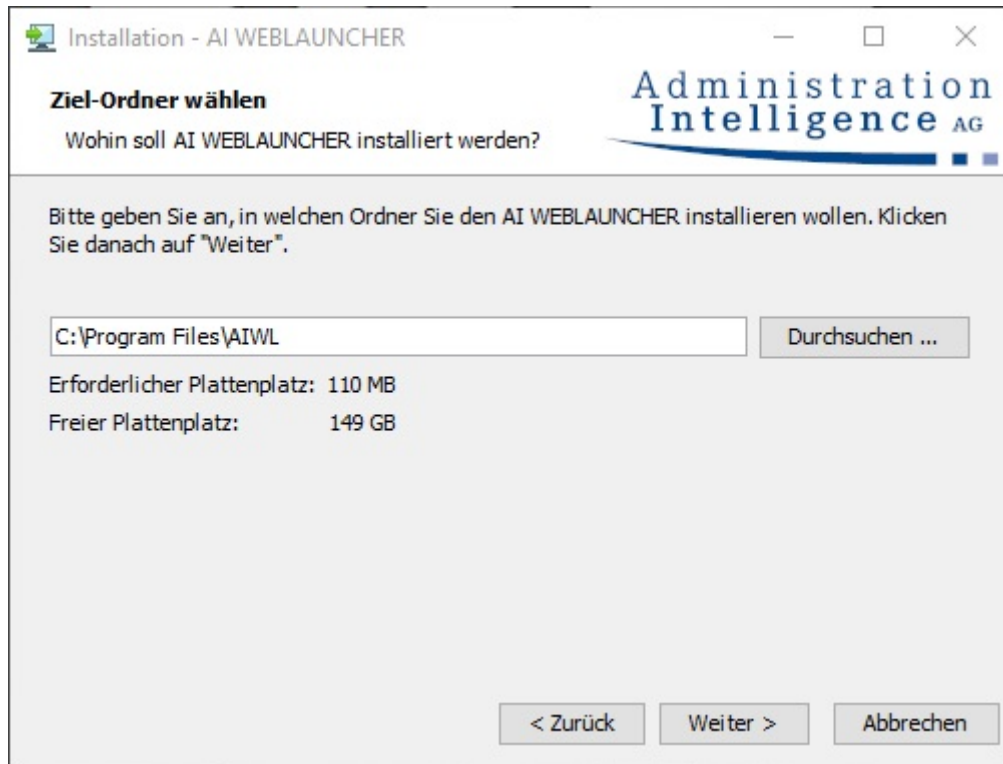


Abbildung 3: Auswahl des **AI WEBLAUNCHER** Installationsverzeichnisses

AI WEBLAUNCHER wird nun in das angegebene Verzeichnis installiert.

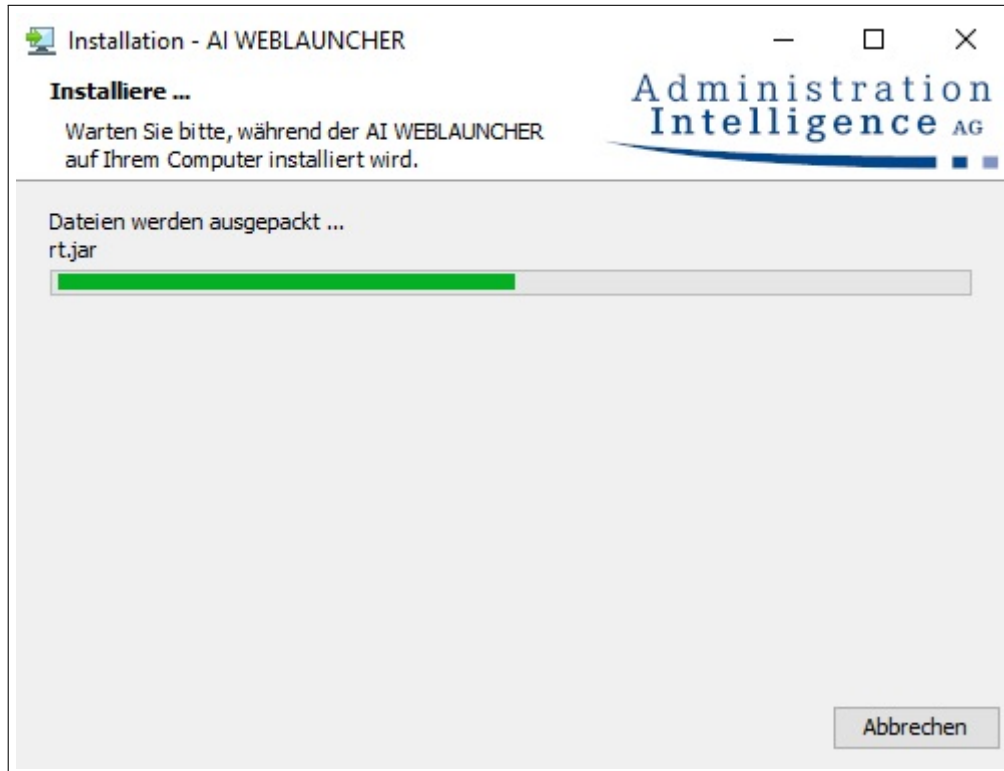


Abbildung 4: AI WEBLAUNCHER Installation

AI WEBLAUNCHER ist nun installiert und die gewünschte Anwendung der Administration Intelligence AG kann gestartet werden.



Abbildung 5: Abschlussbildschirm der **AI WEBLAUNCHER** Installation

2.2 Installation ohne grafische Oberfläche

AI WEBLAUNCHER kann auch ohne grafische Oberfläche mithilfe der Kommandozeile installiert werden. Dabei werden drei verschiedene Möglichkeiten unterstützt. Für die nachfolgenden Beispiele wird exemplarisch eine 64bit Installation für Windows verwendet.

2.2.1 Fragen in der Kommandozeile beantworten

Über den Befehl `start /wait AI_WEBLAUNCHER64bit.exe -c` kann die Installation von **AI WEBLAUNCHER** über die Kommandozeile gestartet werden. Dort müssen, wie in der Installation mit grafischer Oberfläche, alle Fragen beantwortet werden.

2.2.2 Konfiguration als Parameter übergeben

Alternativ kann man das Installationsverzeichnis, in welchem **AI WEBLAUNCHER** installiert werden soll, als Parameter an die Installationsdatei übergeben werden. Der Befehl dafür lautet:

```
start /wait AI_WEBLAUNCHER64bit.exe -q -dir <Installationsverzeichnis>
```

2.3 Starten von Anwendungen mittels AI WEBLAUNCHER

Nachdem die Installation von **AI WEBLAUNCHER** abgeschlossen wurde, können die Client-Anwendungen der Administration Intelligence AG erstmalig gestartet werden. Hierzu muss über einen Browser der entsprechende Link angeklickt werden, wodurch die Installation der Client-Anwendung gestartet wird.

2.3.1 Mime-Type-Verknüpfung

Die Installation des **AI WEBLAUNCHER** erzeugt auf dem System eine Verknüpfung mit dem Mime-Type `application/x-aiweblaunch` (Dateiendung `aiweblaunch`), sodass diese Dateien automatisch durch **AI WEBLAUNCHER** verarbeitet werden.

2.3.2 Speicherort

Wenn die Installation abgeschlossen ist und die benötigten Voreinstellungen vorgenommen wurden, können die Anwendungen gestartet werden. Je nach Betriebssystem werden die notwendigen Komponenten in den unten genannten Speicherort heruntergeladen:

Betriebssystem	Speicherort
Windows	%LOCALAPPDATA%\AI\PRODUCTNAME\HOSTNAME
Linux	user.home/AI/PRODUCTNAME/HOSTNAME
macOS	user.home/Library/AI/PRODUCTNAME/HOSTNAME

Es handelt sich hier bei PRODUCTNAME und HOSTNAME um Platzhalter. PRODUCTNAME ist z. B. für **AI VERGABEMANAGER** durch **VM** und für **AI BIETERCOCKPIT** durch **BCockpit** zu ersetzen. HOSTNAME muss durch die URL des Servers ersetzt werden.



Beispiel für einen Speicherort für den **AI VERGABEMANAGER**:

C:\Users\jdoe\AppData\Local\AI\VM\www.vergabemanager.de\

Beispiel für einen Speicherort für das **AI BIETERCOCKPIT**:

C:\Users\jdoe\AppData\Local\AI\BCockpit\www.vergabepattform.ai-ag.de\

2.3.2.1 Logausgaben

Im Speicherort der Applikation können in der Datei „launcher.log“ die Logausgaben des Programmstarts gefunden werden. Der Speicherort der Logdateien der gestarteten Anwendung ist unverändert.

2.3.2.2 Neuen Download der Applikation erzwingen

Wenn ein erneuter Download der Client-Anwendung erzwungen werden soll, können die Dateien im Speicherort gelöscht werden (Löschen des Cache). **AI WEBLAUNCHER** wird automatisch alle benötigten Dateien erneut vom Applikationsserver herunterladen.

WICHTIG: Sollten Proxyeinstellungen vorgenommen oder SSL-Zertifikaten dauerhaft vertraut worden sein, dürfen die Dateien „proxy.txt“ (Proxy-Einstellungen) und „usertrustedcerts“ (dauerhaft vertrauenswürdige SSL-Zertifikate) nicht gelöscht werden!

2.3.3 Verwendete Version von AI WEBLAUNCHER auslesen

Wenn innerhalb einer Client-Applikation ein Fehlerbericht erstellt wird, kann in der Datei „SystemInfo.html“ unter dem Punkt „Program information“ die verwendete Version des **AI WEBLAUNCHER** ausgelesen werden.

2.3.4 Besonderheiten unter Windows

Benutzerkontensteuerung

UAC beschreibt bewährte Methoden, Standort, Werte, Gruppenrichtlinien-Verwaltungskonsole und Sicherheitsaspekte für die Benutzerkontensteuerung. UAC ist unverzichtbar für alle

Umgebungen, in denen mit administrativen Rechten gearbeitet werden muss und erhöht in diesen die Sicherheit. Der entscheidende Punkt ist, dass administrative Rechte immer erst nach einer Zustimmungsabfrage zur Verfügung stehen und nicht automatisch benutzt werden können. Außerdem sind die UAC durchsetzenden Funktionalitäten ideal geeignet, um die Rechte von nicht vertrauenswürdigen Prozessen innerhalb einer Nutzersitzung einzuschränken. Dies gilt vor allem für alle Prozesse, die mit dem Internet kommunizieren.

3 Netzwerkstruktur und Sicherheit

3.1 Proxy-Dialog

Gelingt es nicht, die Verbindung aufzubauen, erscheint ein Dialog zur Eingabe der Proxy-Konfigurationsdaten. Erfassen Sie Hostnamen bzw. IP-Adresse und den Port des Proxy-Servers. Mit der Bestätigung werden diese Informationen für künftige Starts gespeichert.



Abbildung 6: Proxy ohne Authentisierung

Falls für den Proxy eine Authentisierung erforderlich ist, muss der entsprechende Haken aktiviert werden, sodass der Benutzername und das Passwort ebenfalls eingetragen werden können.

3.2 Server-Authentisierung-Dialog

Wird während der Datenverbindung durch den **AI WEBLAUNCHER** eine Server-Authentisierungsanfrage erkannt, so wird der Anwender nach den Zugangsdaten gefragt.

Mit der Bestätigung werden diese Informationen für künftige Verbindungen gespeichert.

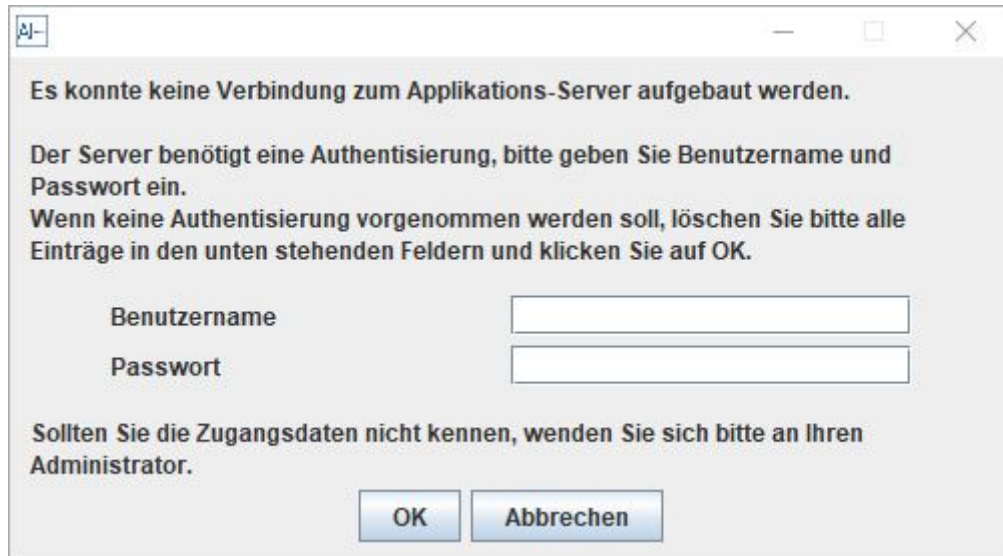


Abbildung 7: Ermittlung der Server-Zugangsdaten für **AI WEBLAUNCHER**

3.3 SSL-Dialog

Ist die Verbindung zu dem Applikationsserver durch ein nicht vertrauenswürdiges SSL-Zertifikat geschützt, wird der Benutzer gefragt ob er diesem trotzdem vertrauen möchte. Dabei werden Informationen wie der Aussteller, die Zertifizierungsstelle und der Gültigkeitszeitraum angezeigt.

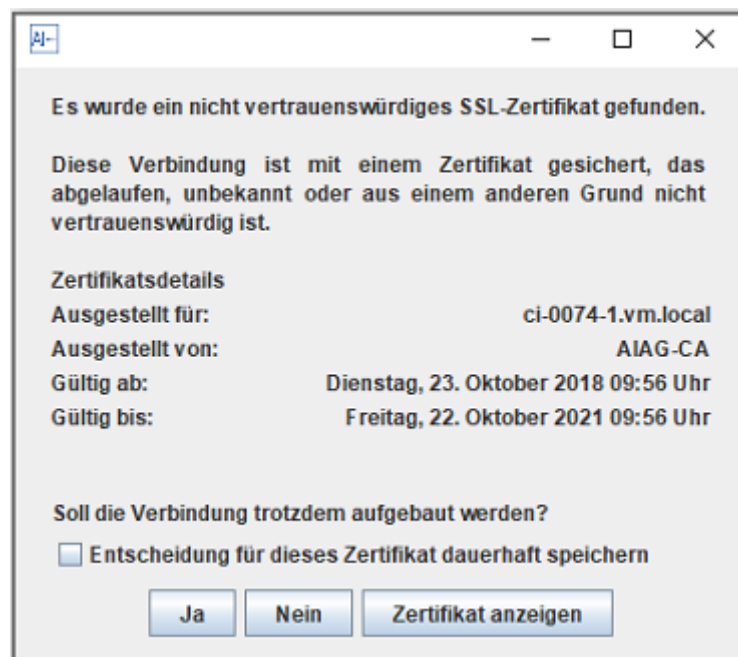


Abbildung 8: SSL Dialog

Durch bestätigen des Dialogs wird dem SSL-Zertifikat temporär vertraut und eine Verbindung

zum Applikationsserver hergestellt. Der Benutzer kann seine Entscheidung dauerhaft speichern, indem er den Haken „Entscheidung für dieses Zertifikat dauerhaft speichern“ setzt und den Dialog bestätigt.

3.4 Auslieferung von Proxy-, Server- und SSL-Einstellungen durch zentrale Verteilung

Um die Proxy-, Server- und SSL-Einstellungen (siehe Kapitel 3.1, 3.2 und 3.3) zentral an mehrere Arbeitsplatzrechner auszuliefern, installieren Sie zunächst den **AI WEBLAUNCHER** und starten Sie die betreffende Client-Anwendung einmalig. Nach der Beantwortung der in Kapitel 3.1, 3.2 und 3.3 beschriebenen Dialoge finden Sie die Einstellungen in den Konfigurationsdateien „proxy.txt“ (Proxy-Einstellungen), „credentials.txt“ (Proxy-Authentifizierung), „servercredentials.txt“ (Server-Authentifizierung) und „usertrustedcerts“ (dauerhaft vertrauenswürdige SSL-Zertifikate). Diese Dateien können nun mittels zentraler Verteilung an den Speicherort der jeweiligen Applikationen (siehe Kapitel 2.3.2) gelegt werden, so dass sie beim Start einer Applikation automatisch verwendet werden. Das in der Tabelle in Kapitel 2.3.2 genannte Verzeichnis muss für eine zentrale Auslieferung der Konfigurationsdateien manuell angelegt werden, falls die Client-Anwendung von diesem Rechner bisher noch nicht gestartet wurde.

Sollte kein Zugriff auf den Speicherort der Applikation möglich sein, können die Konfigurationsdateien auch auf oberster Ebene im Installationsverzeichnis des **AI WEBLAUNCHER** gelegt werden. Bei den Dateien „proxy.txt“, „credentials.txt“ und „servercredentials.txt“ ist zu beachten, dass der Hostname mit im Namen der Datei stehen muss. Z. B. heißt die Proxykonfiguration für eine Applikation, die auf „www.ai-ag.de“ gehostet wird, „proxy_ai-ag.de.txt“.

Um ein SSL-Zertifikat manuell in die Datei „usertrustedcerts“ aufzunehmen, öffnen Sie diese bitte mit einem Texteditor und tragen Sie die Signatur des betreffenden SSL-Zertifikats als hexadezimale Zeichenkette ein. Um die Signatur eines Zertifikates zu ermitteln, können Sie beispielsweise die Eigenschaften des Zertifikates mit dem Firefox Browser anzeigen lassen.

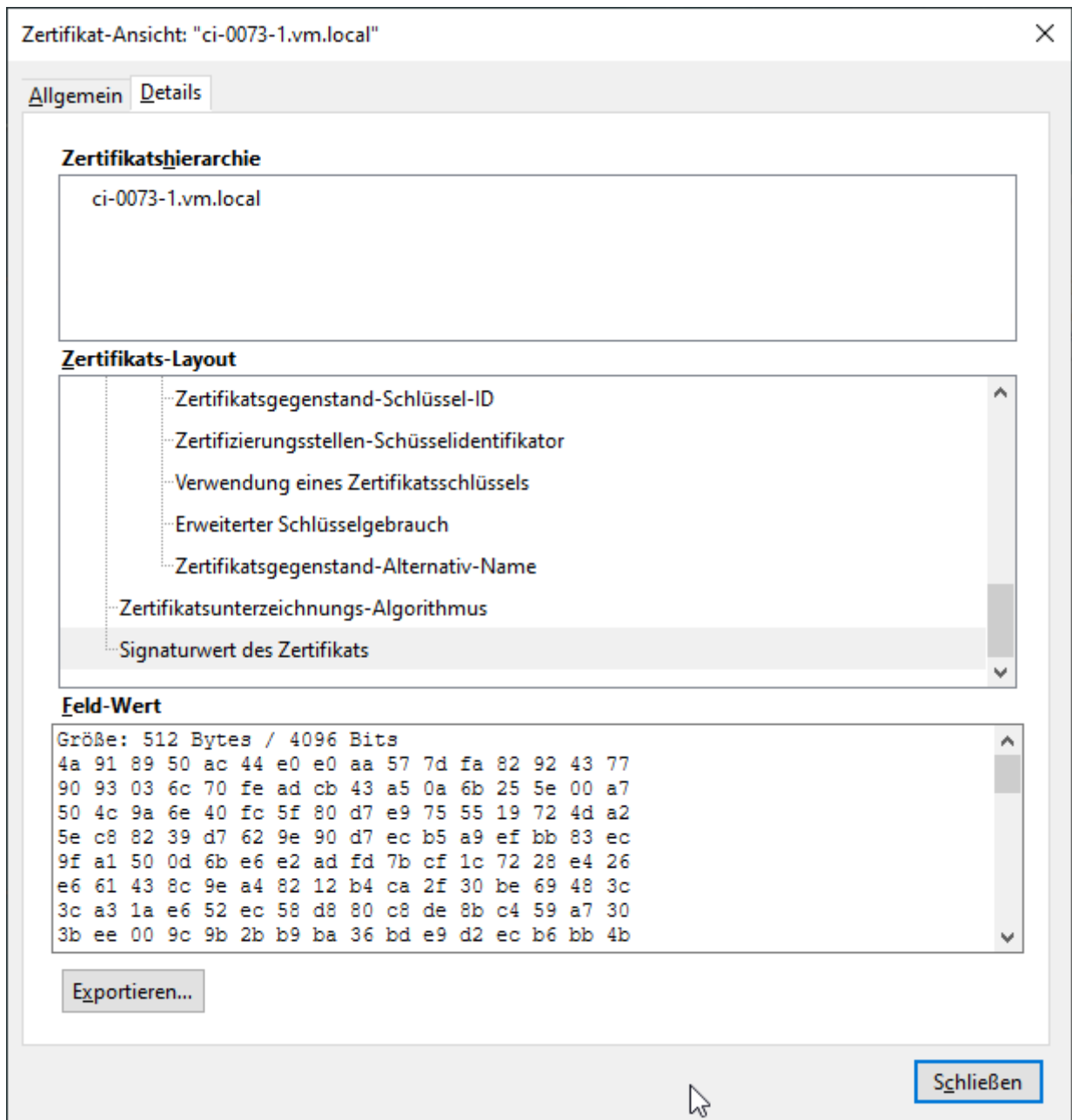


Abbildung 9: SSL Zertifikatseigenschaften im Firefox Browser

Eine weitere Alternative zur Ermittlung der Signatur ist die Nutzung des Tools OpenSSL mit folgendem Kommando:

```
openssl x509 -in „c:\Users\ffrankenberger\Desktop\ssl_73_base64.cer“ -text
```

```

Administrator: Eingabeaufforderung
Digital Signature, Key Encipherment
X509v3 Extended Key Usage:
  TLS Web Server Authentication
X509v3 Subject Alternative Name:
  DNS:ci-0073-1.vm.local
Signature Algorithm: sha256WithRSAEncryption
4a:91:89:50:ac:44:e0:e0:aa:57:7d:fa:82:92:43:77:90:93:
03:6c:70:fe:ad:cb:43:a5:0a:6b:25:5e:00:a7:50:4c:9a:6e:
40:fc:5f:80:d7:e9:75:55:19:72:4d:a2:5e:c8:82:39:d7:62:
9e:90:d7:ec:b5:a9:ef:bb:83:ec:9f:a1:50:0d:6b:e6:e2:ad:
fd:7b:cf:1c:72:28:e4:26:e6:61:43:8c:9e:a4:82:12:b4:ca:
2f:30:be:69:48:3c:3c:a3:1a:e6:52:ec:58:d8:80:c8:de:8b:
c4:59:a7:30:3b:ee:00:9c:9b:2b:b9:ba:36:bd:e9:d2:ec:b6:
bb:4b:0a:7c:40:6b:46:3b:ad:df:b5:88:30:98:f4:9c:a9:a4:
df:72:0b:f2:2a:64:a3:f1:c4:54:fd:8a:46:85:2c:4b:a7:bb:
f8:b3:6a:72:fd:7b:36:d2:85:be:e9:6c:6b:ac:20:9f:45:72:
31:a6:2e:f2:24:4a:97:32:c0:3e:ce:57:9d:1b:f8:11:a4:ee:
9b:54:87:ac:6b:33:74:a7:a4:33:a2:39:35:94:d0:60:a2:1c:
f8:60:4c:5d:06:97:ce:05:c2:46:a3:8d:63:9c:43:d0:55:7b:
94:a2:9f:cb:b9:68:b9:05:4d:43:88:47:42:a2:a6:ba:ae:18:
f8:32:dc:fe:66:cc:08:7e:3a:6a:6b:2d:0c:20:15:7f:94:58:
a2:33:de:b2:13:f8:11:82:07:23:db:87:0b:fe:51:b5:bd:19:
c5:83:70:39:98:fc:7d:0b:a5:df:46:ed:ff:e0:01:81:bd:f4:
76:41:47:c6:96:71:f5:95:7f:a2:83:0f:4b:63:8e:c3:2e:ef:
fe:46:67:41:76:5a:2b:fb:5a:0b:cc:14:b3:88:70:30:24:88:
87:b3:95:80:39:0f:3b:5c:e4:34:3a:b8:b6:3c:e6:7c:82:f1:
0b:c4:30:2d:f1:fa:18:b9:c0:3f:76:1b:e9:7c:09:91:f5:fa:
06:7e:8e:be:2b:f8:bc:57:10:2b:05:ae:57:fa:21:d3:74:22:
c8:91:7c:71:ca:71:ac:70:01:73:c3:af:af:09:bc:14:48:b4:
93:d8:a1:d3:fd:9c:5b:be:8d:06:5f:dc:17:50:2f:cc:3b:c9:
c0:3a:23:a0:d1:56:6d:e4:5d:ff:fe:37:1f:92:57:82:7d:74:
42:bc:52:17:91:66:37:19:bc:cc:c1:c5:67:43:6c:ea:2a:91:
d2:95:40:c6:ad:31:53:a4:48:ee:1b:c5:9e:77:7f:be:84:a3:
18:8b:a6:5d:85:70:b7:e7:d9:c0:bc:0c:53:e0:00:cd:2f:8b:
db:54:0f:38:d2:fd:ec:bc
-----BEGIN CERTIFICATE-----
MIIFbDCCA1SgAwIBAgICEeIwDQYJKoZIhvcNAQELBQAwXDELMAkGA1UEBhMCREUx
CzAJBgNVBAgTAkZJMRIwEAYDVQQHEw1XdWVyeMj1cmcxDDAKBgNVBAoTAlBURzEM
MAoGA1UECXMdMW1NBMRwDgYDVQQDEwdBSUFHLUNBMB4XDTE5MDQyMzIxMDMzOFoX
DTIyMDQyMjIxMDMzOFowXzELMAkGA1UEBhMCREUxZDZANBgNVBAgMBkRzZWVyejES
MBAGA1UEBwwJVjV3V1cnpidXJnMQ4wDAYDVQQQLDAVBSS1BRzEbMBkGA1UEAwwSY2kt
MDA3My0xLnZtLmxvY2FsMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
v16FeUpDoCwwd0uY3ykfgs7/UwprX088FLGwTRjt0TzmyiD6RJ4We66WHw/JO39c

```

Abbildung 10: SSL Zertifikatseigenschaften in der Kommandozeile

Das Zertifikat ssl_73_base64.cer muss dabei in Base64-Kodierung gespeichert sein. Bitte entfernen Sie beim Übernehmen einer Signatur in die Datei „usertrustedcerts“ jegliche Leerzeichen, Zeilenumbrüche oder andere Trennzeichen wie Doppelpunkte. Um mehrere SSL-Zertifikate als vertrauenswürdig einzustufen, können auch mehrere Signaturen eingetragen werden. Dabei muss jede Signatur in einer neuen Zeile hinterlegt werden.

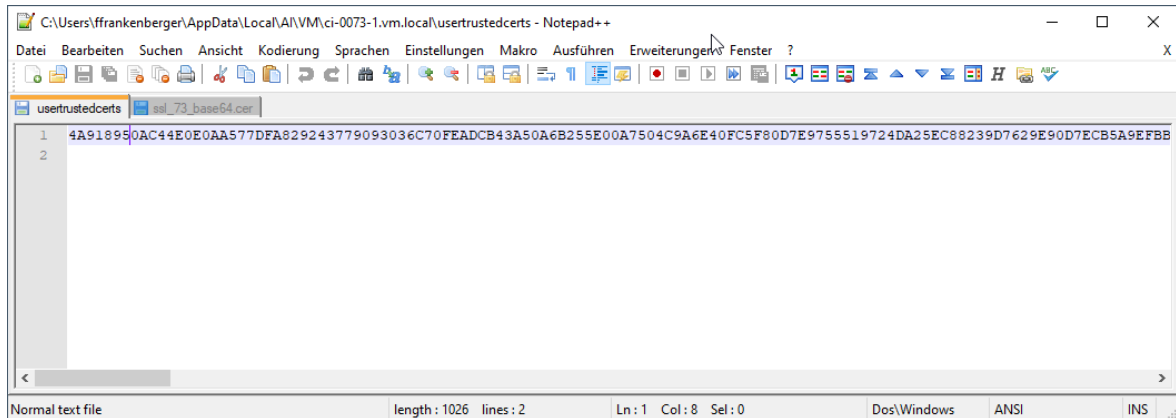


Abbildung 11: usertrustedcerts Datei