Governikus KG

Governikus Signer WebEdition

Benutzerhandbuch

Governikus Signer WebEdition

Governikus Signer WebEdition, Release 2.9.0

Inhaltsverzeichnis

1 Rechtliche Informationen und weitere Hinweise

Obwohl diese Produktdokumentation nach bestem Wissen und mit größter Sorgfalt erstellt wurde, können Fehler und Ungenauigkeiten nicht vollständig ausgeschlossen werden. Eine juristische Verantwortung oder Haftung für eventuell verbliebene fehlerhafte Angaben und deren Folgen wird nicht übernommen. Die in dieser Produktdokumentation enthaltenen Angaben spiegeln den aktuellen Entwicklungsstand wider und können ohne Ankündigung geändert werden. Künftige Auflagen können zusätzliche Informationen enthalten. Technische und orthografische Fehler werden in künftigen Auflagen korrigiert.

Sofern in dem vorliegenden Produkt für Personen ausschließlich die männliche Form benutzt wird, geschieht dies nur aus Gründen der besseren Lesbarkeit und hat keinen diskriminierenden Hintergrund.

2 Einleitung

Die Governikus Signer WebEdition ist eine Software, die auf einer Webseite oder in einer Fachanwendung üblicherweise über einen Link gestartet wird. Die Governikus Signer WebEdition ist ein eigenständiges Programm.

	**Hinweis**: Im Folgenden wird die **Governikus Signer WebEdition** mit **WebEdition** abgekürzt.

Funktionsumfang

Die WebEdition ermöglicht es Ihnen, Dateien elektronisch zu signieren und zu ver- oder entschlüsseln.

- **Signieren**: Mit einem Kartenleser und einer Signaturkarte, können Sie mit der WebEdition Dateien qualifiziert elektronisch signieren. Für Siegelkarten ist dieser Vorgang technisch identisch, siehe dazu das nächste Kapitel. Zudem können Sie auch fortgeschrittene elektronische Signaturen mit einer Schlüsselspeicherdatei (Keystore) erstellen.
- **Verschlüsseln**: Sie können Dateien mit einem Passwort, dem öffentlichen Schlüssel eines Software-Zertifikats oder mit dem öffentlichen Schlüssel eines Zertifikats von einer Signaturkarte verschlüsseln.
- **Entschlüsseln**: Sie können Dateien mit einem Passwort, dem privaten Schlüssel eines Software-Zertifikats oder mit dem privaten Schlüssel eines Zertifikats von einer Signaturkarte entschlüsseln.

2.1 Signaturkarten und Siegelkarten

Mit der WebEdition kann mit einem Chipkartenleser und einer Signaturkarte eine qualifizierte elektronische Signatur für eine Datei erstellt werden. Ebenso kann mit der WebEdition mit einem Chipkartenleser und einer Siegelkarte ein qualifiziertes elektronisches Siegel für eine Datei erstellt werden. Technisch sind diese Vorgänge identisch. Qualifizierte elektronische Signatur und qualifiziertes elektronisches Siegel haben jedoch unterschiedliche Rechtswirkungen.

- **Qualifizierte elektronische Signatur**: Die qualifizierte elektronische Signatur ist der handschriftlichen Unterschrift rechtlich gleichgestellt.
- **Qualifiziertes elektronisches Siegel**: Die Frage nach der rechtlichen Wirkung eines qualifizierten elektronischen Siegels kann von Seiten der Governikus KG für kein Szenario beantwortet werden. Dies ist unter anderem abhängig vom Siegelzweck und davon, was nach dem Siegeln mit der gesiegelten Datei geschehen soll. Hier greifen in unterschiedlichen Kontexten und Fachverfahren unterschiedliche Gesetze, Verordnungen oder Regelungen. Eine Bewertung der Rechtswirkung eines qualifizierten elektronischen Siegels muss der Fachjurist Ihrer Institution abgeben.

	Hinweis: Wenn im Folgenden von Signaturkarten und qualifizierten elektronischen Signaturen die Rede ist, gelten die beschriebenen Vorgänge **technisch** genauso für Siegelkarten und qualifizierte elektronische Siegel. Eine Ausnahme stellen Attributzertifikate dar, die es nur für Signaturen und nicht für Siegel gibt.

2.2 Das Angebot Ihres Dienstanbieters

Ihr Dienstanbieter, der die WebEdition bereitstellt, hat die Möglichkeit, dieses Programm vielfältig einzustellen, sodass es genau auf die Bedürfnisse und Anforderungen der vorliegenden Fachanwendung oder Webseite eingestellt ist. Die WebEdition hat unterschiedliche Dialogseiten.

Ausgegraute oder ausgeblendete Dialogseiten

Dialogseiten können ganz oder teilweise ausgegraut sein. In diesem Fall können Sie auf dieser Seite nur wenige oder keine Einstellungen vornehmen und sich nur über die festgelegten Einstellungen informieren. Oder Dialogseiten sind vollständig ausgeblendet. In diesem Fall hat Ihr Dienstanbieter die auf diesen Seiten möglichen Einstellungen bereits fest eingestellt und bietet den Dialog nicht mehr an.

2.3 Prüfung der Vertrauenswürdigkeit

Wenn Sie die Anwendung WebEdition aus dem Internet aufrufen, achten Sie darauf, dass dies nur über eine gesicherte und vertrauenswürdige Verbindung erfolgt. Dass eine gesicherte Verbindung verwendet wird, erkennen Sie in Ihrem Browser daran, dass die Adresse der Webseite mit `https://` beginnt, bzw. zusätzlich das Symbol eines Schlosses dargestellt wird. Die Vertrauenswürdigkeit können Sie anhand des Zertifikates der Webseite prüfen, von der Sie die Anwendung WebEdition aufrufen. Informationen zur Gültigkeit und Vertrauenswürdigkeit des Zertifikats erhalten Sie über Ihren Browser, siehe nächste Abbildung.

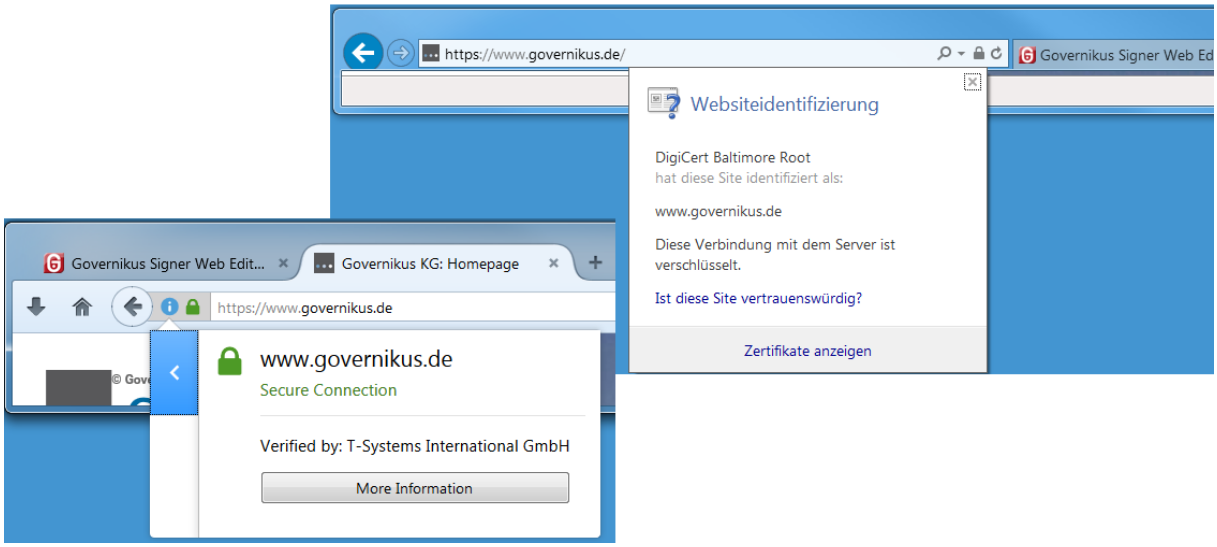


Abbildung 1: Zertifikatsinformationen am Beispiel Firefox und Internet Explorer

3 Betriebsvoraussetzungen

Bitte lesen Sie den folgenden Warnhinweis vollständig.

	**Achtung**: Der Dienstanbieter, über dessen Seiten Sie die WebEdition aufrufen, kann diese Software vielfältig einstellen und anpassen. Im Folgenden werden alle Möglichkeiten beschrieben, die die WebEdition bietet. Der Dienstanbieter bietet immer nur seine Auswahl an. Abhängig von dieser Auswahl stehen also bestimmte, nachfolgend beschriebene Möglichkeiten nicht zur Verfügung oder sind ausgeblendet.

Unterstützten Betriebssysteme, Chipkartenleser und Signaturkarten

Die detaillierte Auflistung der Unterstützten Betriebssysteme, Chipkartenleser und Signaturkarten finden Sie in dem separaten Dokument "Governikus-Signer-WE-Systemanforderungen.pdf".

3.1 Unterstützte Betriebssysteme

Unterstützte Betriebssysteme

Die WebEdition kann auf den folgenden Betriebssystemen eingesetzt werden:

- **Windows**: 7, 8, 8.1 und 10

	**Hinweis**: Auf allen aufgeführten Betriebssystemen müssen aktuelle Service Packs installiert sein.

3.2 Ausstattungsanforderung

Signieren

Für das Signieren benötigen Sie:

- eine gültige Schlüsselspeicherdatei, (Keystore-Datei). Die Dateiendung ist gewöhnlich `.p12` oder `.jks` oder eine gültige Signaturkarte.
- einen Chipkartenleser, wenn sofern eine Signaturkarte verwendet wird.

Verschlüsseln

Für das Verschlüsseln benötigen Sie:

- ein X509v3 Zertifikat des Empfängers als Softwarezertifikat (Dateiendung ist gewöhnlich `.cer` oder `.crt`) oder gespeichert auf einer Signaturkarte.
- einen Chipkartenleser, sofern das Zertifikat von einer Signaturkarte verwendet wird.

Entschlüsseln

Für das Entschlüsseln benötigen Sie:

- einen passenden privaten Schlüssel gespeichert in einer Schlüsselspeicherdatei (PKCS12-Keystore, Dateiendung ist für gewöhnlich `.p12`) oder auf einer Signaturkarte.
- einen Chipkartenleser, sofern der Schlüssel von einer Signaturkarte verwendet wird.

Eine Aufstellung aller unterstützten Chipkartenleser, unterstützten Signaturkarten sowie unterstützte Kombinationen von Betriebssystem, Chipkartenleser und Signaturkarten finden Sie im Kapitel 4 des Dokuments `Governikus-Signer-WE-Systemanforderungen.pdf`.

Proxy

Die WebEdition funktioniert unabhängig von möglicherweise vorhandenen Proxy-Server. sollte die WebEdition in einer Umgebung ausgeführt werden, die hinter einem Proxy liegt, werden diese Einstellungen für jeden Aufruf ermittelt und berücksichtig.

3.3 Protokolle

Protokolldateien

Die WebEdition protokolliert Ereignisse in sogenannten Log-Dateien:

- Fehlerprotokolldateien haben die Bezeichnung `<Zufallszahl>.err.log`
- Ausgabeprotokolldateien haben die Bezeichnung `<Zufallszahl>.out.log`

In Fehlerprotokolldateien werden Warnungen und Fehler protokolliert, die während der Programmausführung ausgegeben werden.

In Ausgabeprotokolldateien werden Ereignisse protokolliert, die während der Programmausführung ausgegeben werden. Dieses Protokoll entspricht der Ausgabe, die zuvor in einem Kommandofenster ausgegeben wurde.

Fehlerfall

Bei einem Fehler und inkorrektem Verhalten der WebEdition können Protokolldateien bei der Fehlersuche helfen. Sie finden diese Dateien im temporären Verzeichnis des Benutzers. Beispiel für Windows: `C:\Users\<Ihr-Benutzername>\AppData\Local\Temp\Governikus KG\ GovernikusSignerWebEdition`

4 Installation

Damit die WebEdition von einer Fachanwendung oder über eine Webseite aufgerufen werden kann, muss die WebEdition zuerst lokal auf dem PC des Anwenders installiert werden. Diese Kapitel erklärt die Installation auf einem Windows Betriebssystem mit der Microsoft Software Installationsdatei (Dateiendung `.msi`).

	**Hinweis**: Die WebEdition kann nicht als Programm von Ihrem PC gestartet werden. Die WebEdition wird immer über eine Fachverfahren/ein Webportal gestartet.

Aufruf des Installers

Die Installation wird durch einen Doppelklick auf die `.msi`-Datei gestartet:

`GovSignerWebEdition_<Versionsnummer>.msi`

Start des Setup Assistenten

Klicken Sie auf "Weiter"

Abbildung 2: Start des Setup Assistenten

Lizenzvereinbarung

Lesen Sie die Lizenzvereinbarung, wählen Sie "Ich stimmte der Lizenzvereinbarung zu" und klicken Sie dann auf "Weiter".

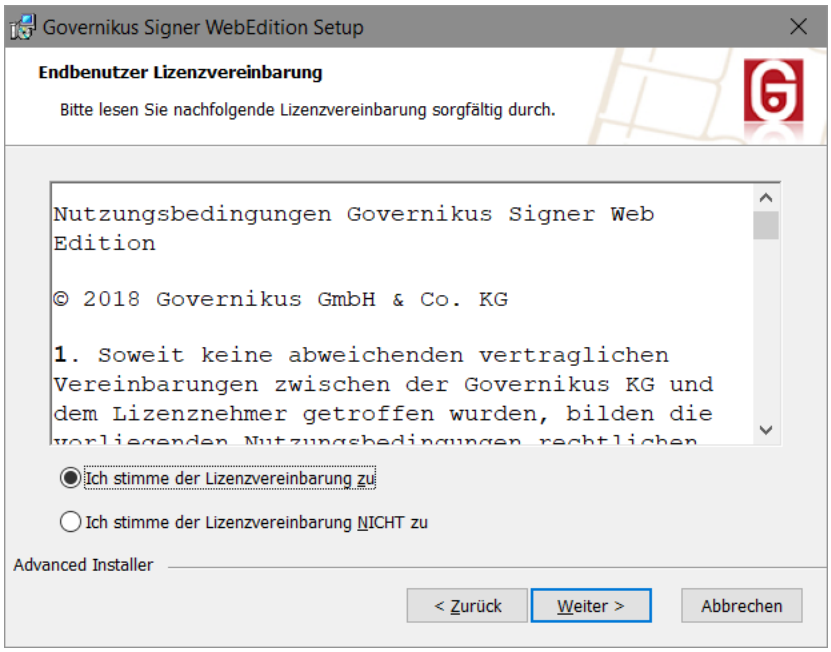


Abbildung 3: Dialogseite mit Lizenzvereinbarung

Installationsverzeichnis wählen

Sie können auf dieser Seite ein anderes Installationsverzeichnis wählen. Wir empfehlen die Vorgabe zu übernehmen. Klicken Sie auf "Weiter".

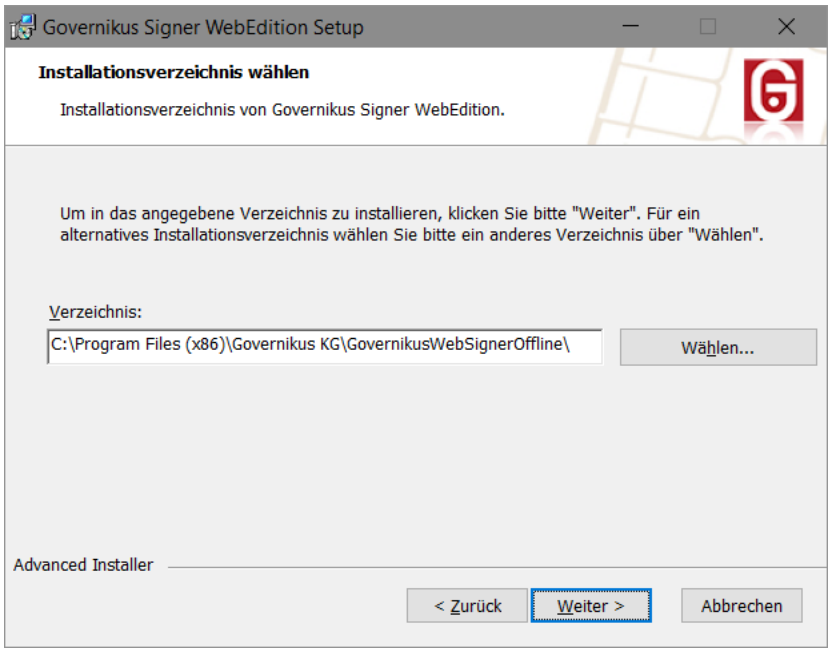


Abbildung 4: Dialogseite Installationsverzeichnis wählen

Installation bestätigen

Klicken Sie auf "Installieren", um den Installationsvorgang zu starten.

Abbildung 5: Dialogseite Installation bestätigen

Statusangaben während der Installation

Diese Dialogseite zeigt den Installationsvorgang an.

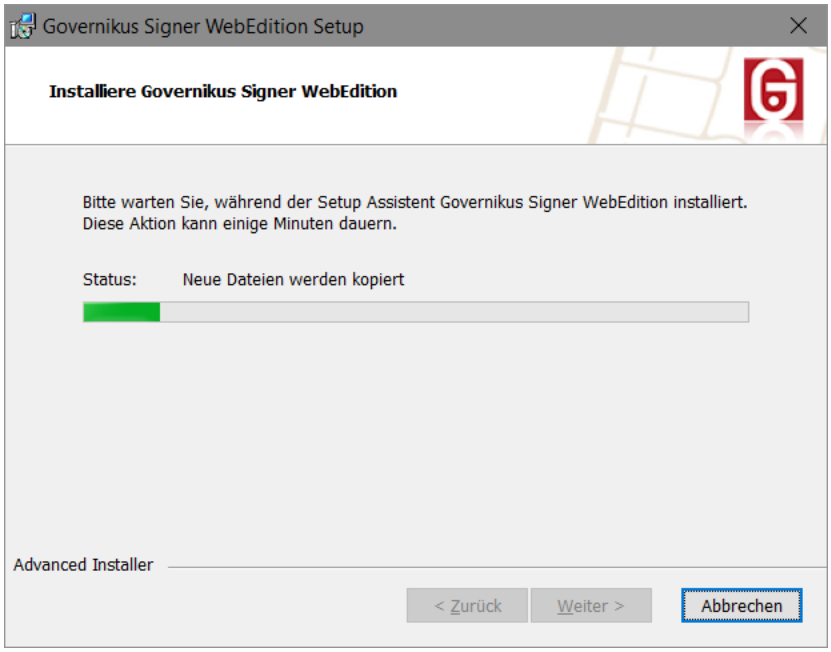


Abbildung 6: Statusangaben während der Installation

Fertigstellen

Das Ende des Installationsvorgangs wird in einem eigenen Dialogfenster angezeigt. Klicken Sie auf "Fertigstellen", um die Installation abzuschließen. Damit ist die Installation vollständig und die WebEdition kann von Fachanwendungen oder Webseiten für die Funktionen Signieren, Ver- und Entschlüsseln aufgerufen werden.

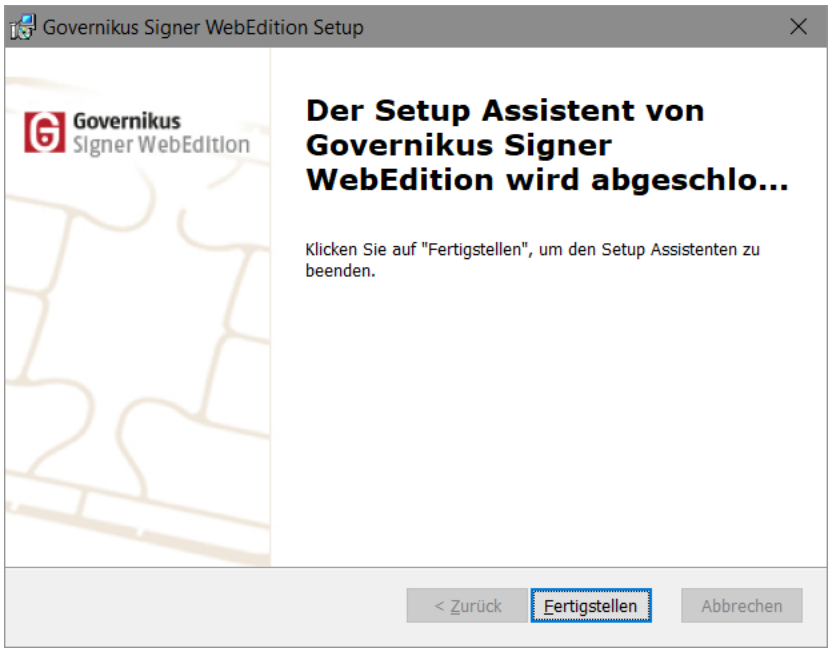


Abbildung 7: Dialogseite Fertigstellen

5 Arbeitsabläufe

Im Folgenden werden die Arbeitsabläufe für das Signieren, Ver- und Entschlüsseln kurz erklärt. Diese Erklärungen geben einen kurzen Überblick über die jeweiligen Funktionen. Die konkrete Benutzung dieser Funktionen mit der WebEdition ist in nachfolgenden Kapiteln erklärt.

5.1 Arbeitsablauf Signieren

Aufruf der WebEdition

Beim Aufruf über einen Button oder einen Link in einer Fachanwendung oder auf einer Webseite werden der WebEdition bereits eine oder mehrere Dateien übergeben, die Sie signieren sollen. Dies sind üblicherweise Dateien, bei denen Sie entweder die Korrektheit des Inhalts durch Ihre elektronische Signatur bestätigen. Oder es sind Dateien oder Formularseiten, in die Sie Daten eingegeben haben, deren Korrektheit Sie durch Ihre elektronische Signatur bestätigen.

Vorgehen nach dem Programmstart

Nachdem das Programm gestartet ist, sehen Sie die Benutzeroberfläche. Auf der linken Seite sind nummerierte und beschriftete Buttons zu sehen, die Sie der Reihe nach anklicken müssen, um die dazugehörige Dialogseite auf der rechten Seite zu bearbeiten.

Dialogseiten bearbeiten

Wie in der Einleitung erklärt, hat Ihr Dienstanbieter die Möglichkeit, der WebEdition vielfältig anzupassen, sodass bis zu vier Dialogseiten verfügbar sind. Wenn nur die Dialogseite "Signieren" zu sehen ist, verfahren Sie wie im Kapitel "Signieren" erklärt. Sollten weitere Dialogseiten verfügbar sein, rufen Sie diese bitte der Reihe nach auf und wählen Sie die Dialogseite Signieren zum Schluss. Sollten weitere Dialogseiten verfügbar sein, sind diese in eigenen Kapiteln erklärt.

Abschluss des Signiervorgangs

Wenn Sie die Dateien signiert haben, die auf der Dialogseite Signieren aufgelistet sind, wird das Programm automatisch geschlossen. Die signierten Dateien werden in dem Verzeichnis abgelegt, das Sie im Dialog "Zielverzeichnis wählen" ausgewählt haben. Sollte dieser Dialog für Sie nicht verfügbar sein, werden die signierten Dateien der aufrufenden Fachanwendung oder so weiterverarbeitet, wie Ihr Dienstanbieter dies eingestellt hat.

Die Benutzeroberfläche

Die folgende Abbildung zeigt die Benutzeroberfläche der WebEdition mit der Dialogseite "Signieren". Bitte beachten Sie, dass abhängig von den Einstellungen Ihres Dienstanbieters bis zu vier Dialogseiten verfügbar sein können.

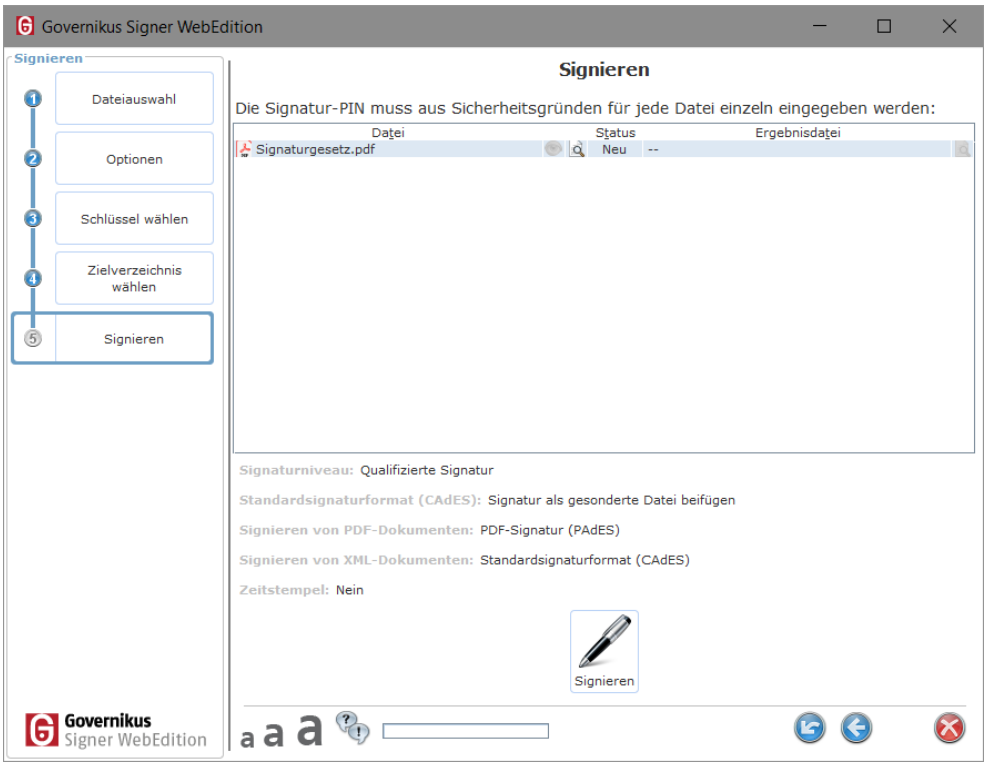


Abbildung 8: WebEdition mit Dialogseite "Signieren"

Wichtiger Hinweis

Wenn Sie Dateien signieren wollen, die von einem Server geladen werden, kann es sein, dass der Diensteanbieter zusammen mit der Datei den Hashwert in die WebEdition herunter lädt (zu Hashwerten lesen Sie bitte auch Kapitel 12.2). Die WebEdition berechnet diesen Hashwert neu und vergleicht ihn mit dem Wert, der vom Server herunterladen wurde. Stimmen diese Werte nicht überein, wurde die Datei zwischen dem Herunterladen der Datei und dem Start der WebEdition sehr wahrscheinlich verändert. Es wird ein Warndialog angezeigt. Die folgende Abbildung zeigt ein Beispiel:

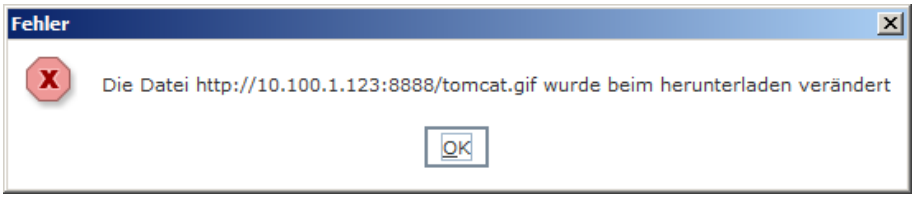


Abbildung 9: Beispielhafter Warndialog bei veränderter Datei

	**Achtung**: Wenn der oben abgebildete Warndialog angezeigt wird, ist die Wahrscheinlich sehr hoch, dass die Datei verändert wurde. In diesem Fall ist es dringend empfohlen, den Signiervorgang abzubrechen!

5.2 Arbeitsablauf Ver- und Entschlüsseln

Arbeitsablauf Verschlüsseln

Abhängig von den Einstellungen, die Ihr Dienstanbieter für die WebEdition getroffen hat, wird beim Aufruf über einen Button oder einen Link in einer Fachanwendung oder auf einer Webseite der WebEdition entweder bereits eine oder mehrere Dateien übergeben oder Sie haben die Möglichkeit, selber Dateien hinzuzufügen. Führen Sie dann die jeweils notwendigen Arbeitsschritte aus.

Verschlüsseln

Verschlüsseln Sie Dateien, so dass sie auch bei Zugriff durch Unbefugte nicht lesbar oder benutzbar sind.

Entschlüsseln

Entschlüsseln Sie Dateien, um diese wieder in einen lesbaren oder benutzbaren Zustand zu überführen.

Vorgehen nach dem Programmstart

Nachdem das Programm gestartet ist, sehen Sie die Benutzeroberfläche. Auf der linken Seite sind nummerierte und beschriftete Buttons zu sehen, die Sie der Reihe nach anklicken müssen, um die dazugehörige Dialogseite auf der rechten Seite zu bearbeiten.

Dialogseiten bearbeiten

Wie in der Einleitung erklärt, hat Ihr Dienstanbieter die Möglichkeit, die WebEdition vielfältig anzupassen, sodass unterschiedlich viele Dialogseiten verfügbar sind. Es können nur die Hauptdialogseiten "Verschlüsseln" oder "Entschlüsseln" verfügbar sein. Es können für jede Funktion aber auch mehrere Dialogseiten angeboten werden. Diese sind in eigenen Kapiteln erklärt.

Abschluss der Funktionsausführung

Nachdem Sie die Dateien verschlüsselt oder entschlüsselt haben, die auf der jeweiligen Dialogseite aufgelistet sind, wird das Programm automatisch geschlossen. Die Dateien werden in dem Verzeichnis abgelegt, das Sie im Dialog "Zielverzeichnis wählen" ausgewählt haben. Sollte dieser Dialog für Sie nicht verfügbar sein, werden die Dateien der aufrufenden Fachanwendung übergeben oder so weiterverarbeitet, wie Ihr Dienstanbieter dies eingestellt hat.

Die Benutzeroberfläche

Die folgende Abbildung zeigt die Benutzeroberfläche der WebEdition beispielhaft mit der Dialogseite "Verschlüsseln". Bitte beachten Sie, dass abhängig von den Einstellungen Ihres Dienstanbieters nur eine oder mehrere Dialogseiten einer Funktion verfügbar sein können.

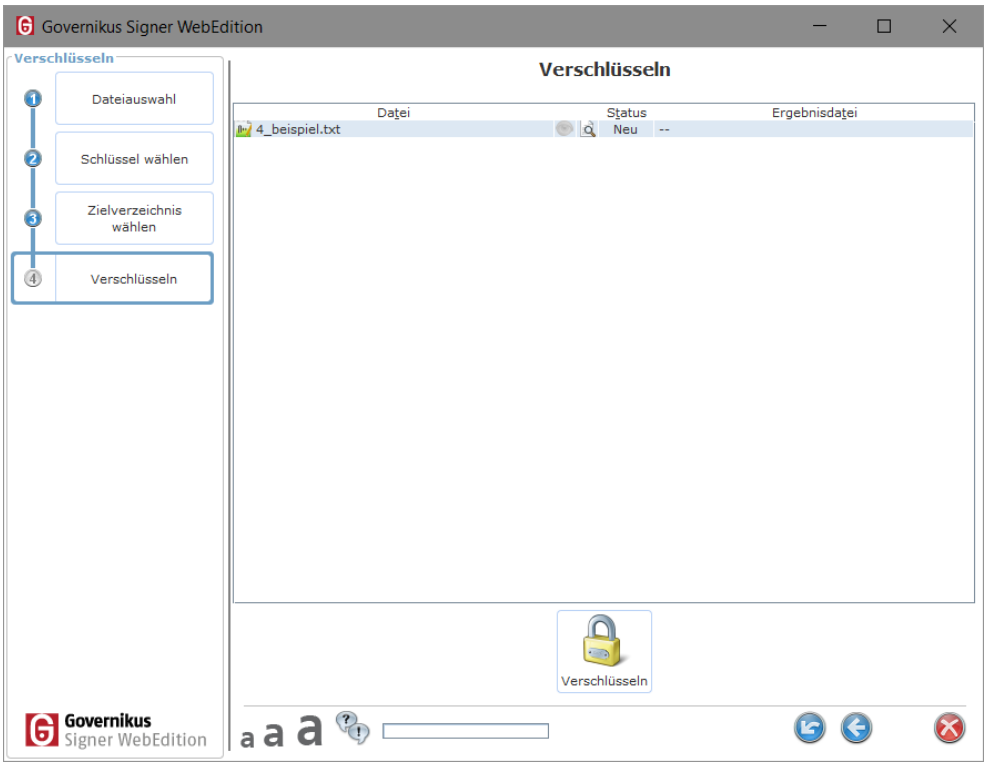


Abbildung 10: Benutzeroberfläche der WebEdition mit der Dialogseite "Verschlüsseln"

5.3 Verfügbare Buttons auf Dialogseiten

-  : Diese drei unterschiedlich großen Buchstaben sind jeweils Buttons, mit denen die Schriftgröße aller Dialogtexte zu "Klein", "Normal" oder "Groß" verändert werden kann.
-  : Mit diesem Button starten Sie die Online-Hilfe.
-  : Mit diesem Button brechen Sie das Programm ab. Danach wird die Fachanwendung angezeigt, oder die Webseite, die Ihr Dienstanbieter für diesen Fall vorgesehen hat.
-  : Wenn Ihr Dienstanbieter die WebEdition so eingestellt hat, dass mehr als eine Dialogseite verfügbar ist, dann gelangen Sie mit diesem Button zur ersten Dialogseite, die zur Verfügung steht.
-  : Wenn Ihr Dienstanbieter die WebEdition so eingestellt hat, dass mehr als eine Dialogseite verfügbar ist, dann gelangen Sie mit diesen Buttons zur vorangegangenen beziehungsweise nachfolgenden Dialogseite.

6 Signieren mit der WebEdition

Im Folgenden werden die Dialoge erklärt, die für die Funktion "Signieren" existieren. Bitte beachten Sie, dass Dialogseiten ganz oder teilweise ausgegraut sein können oder gar nicht angezeigt werden, wenn die dort vorhandenen Einstellungen bereits von Ihrem Diensteanbieter festgelegt wurden.

6.1 Dateiauswahl

Bitte beachten Sie, dass diese Dialogseite möglicherweise nicht angezeigt wird, wenn die zu signierenden Dateien bereits mit dem Start der Anwendung vorgegeben sind. Auf der rechten Seite der Dialogseite finden Sie eine Liste, die anfangs leer ist. Sie können beliebig viele Dateien aus verschiedenen Verzeichnissen auswählen. Sie können der Liste auf zwei Wegen Dateien hinzufügen.

1. Drag-and-drop

Markieren Sie eine oder mehrere Dateien im Dateimanager und ziehen Sie die Auswahl bei gedrückter linker Maustaste in die Liste der WebEdition.

2. Button "Datei hinzufügen"

Mit dem Button "Datei hinzufügen" rufen Sie ein Dialogfenster zur Dateiauswahl auf. Navigieren Sie in das gewünschte Verzeichnis, wählen Sie die gewünschten Dateien aus, und klicken Sie auf "Übernehmen". Die Dateiliste enthält nun Ihre Auswahl.

Mehrere Dateien gleichzeitig auswählen

Es gibt verschiedene Möglichkeiten, im Dateimanager oder im Dialog "Dateien auswählen" mehrere Dateien gleichzeitig auszuwählen.

- **Liste auswählen**: Wenn Sie eine Anzahl von Dateien auswählen, die im Verzeichnis untereinanderstehen, markieren Sie die oberste Datei der gewünschten Liste mit dem Tastaturkürzel "Shift - linker Mausklick" und danach die unterste Datei in der gewünschten Liste mit dem Tastaturkürzel "Shift - linker Mausklick". Die gewählten Dateien sind nun farblich hinterlegt und können durch Ziehen (drag-and-drop im Dateimanager) oder durch den Übernehmen-Button der Liste im Governikus Signer hinzugefügt werden.
- **Mehrere Dateien auswählen**: Wenn Sie mehrere Dateien auswählen wollen, die nicht untereinanderstehen, halten Sie die Taste "Strg" gedrückt und wählen Sie durch Anklicken mit der linken Maustaste alle gewünschten Dateien aus.
- **Alle Dateien auswählen**: Wenn Sie alle Dateien eines Verzeichnisses auswählen wollen, öffnen Sie das Verzeichnis und markieren Sie alle Dateien mit dem Tastaturkürzel "Strg + a".
- **Filter**: Wenn Sie den Dialog zur Dateiauswahl geöffnet haben, können Sie unter "Dateityp" einen Filter für bestimmte Dateiendungen auswählen. Alternativ können Sie in die Zeile "Dateiname" auch direkt einen Filter für Dateiendungen eingeben,

beispielsweise `*.docx`. Mit der Enter-Taste wird die Dateiliste gefiltert. Danach werden in der Dateiauswahl nur noch Dateien mit dieser Dateiendung angezeigt. Diese können Sie ebenso auswählen, wie oben erklärt.

Ausgewählte Dateien entfernen

Sie können einzelne oder mehrere Dateien, die auf der Dialogseite "Dateiauswahl" aufgelistet sind, wieder entfernen. Die Auswahl der zu entfernenden Dateien können Sie in dieser Liste genauso vornehmen wie oben erklärt. Klicken Sie nach Ihrer Auswahl auf den Button "Ausgewählte Dateien entfernen".

Listendarstellung

Alle von Ihnen ausgewählten Dateien werden in einer Liste dargestellt. Die Spalten haben die folgende Bedeutung:

- **Datei**: Zeigt den Dateinamen an. Wenn Sie den Mauszeiger über den Dateinamen legen, wird der vollständige Pfad angezeigt. Über einen Doppelklick kann die Datei angezeigt werden.
-  : Das Augensymbol zeigt an, dass die Datei bereits geöffnet wurde. Das Symbol ist grau, wenn die Datei noch nicht angezeigt wurde.
-  : Über dieses Symbol kann die Datei angezeigt werden. Klicken Sie dazu auf das Symbol. Da die resultierende Aktion abhängig von der ausgewählten Funktion ist, wird das konkrete Verhalten jeweils bei der Erklärung der Funktionen aufgeführt. Hinweis: Dateien, die zum Entschlüsseln ausgewählt wurden, können nicht angezeigt werden.

Sonderfall PDF-Datei

Wenn Sie eine PDF-Datei in die Dateiauswahl aufnehmen, können Sie mit einem Rechtsklick auf die PDF-Datei das Kontextmenü "Signaturfelder anlegen" aufrufen. Das Anlegen von Signaturfeldern ist im Kapitel 6.7 erklärt.

6.2 Optionen einstellen

Bitte beachten Sie, dass Dialogseiten ganz oder teilweise ausgegraut sein können oder gar nicht angezeigt werden, wenn die dort vorhandenen Einstellungen bereits von Ihrem Diensteanbieter festgelegt wurden.

Dialog ausgegraut

Dieser Dialog kann ganz oder teilweise ausgegraut sein.

- **Der Dialog ist vollständig ausgegraut**: In diesem Fall können Sie keine Optionen einstellen. Es wird Ihnen angezeigt, welche Optionen ausgewählt sind. Die Bedeutungen der Optionen werden im nächsten Abschnitt erklärt.
- **Der Dialog ist teilweise ausgegraut**: Die Dialogseite besteht aus den Dialogabschnitten "Standardsignaturformat wählen", "Erweiterte Signatur einbetten" und "Vorhandene Signaturen". Die Dialogabschnitte können jeweils ausgegraut sein, während jeweils andere zur Bearbeitung zur Verfügung stehen. Die Bedeutungen der Optionen werden im nächsten Abschnitt erklärt.

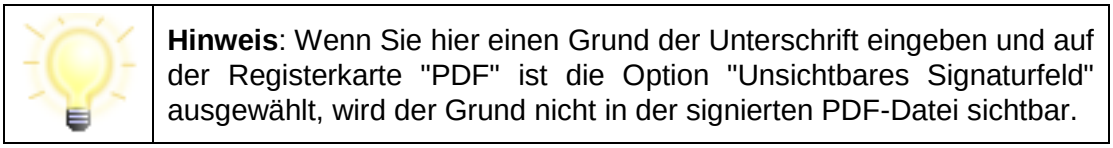
Standardsignaturformat wählen (CAdES)

Dieser Dialogabschnitt kann ausgegraut sein. Die WebEdition unterstützt verschiedene, international standardisierte Formate für elektronische Signaturen.

- **Dokument in Signaturdatei einbetten** (enveloping): Die Datei wird gemäß CAdES-Standard elektronisch signiert. Dabei entsteht genau eine Datei. Die Datei, die signiert werden soll, wird in eine Signaturdatei eingebettet (enveloping). Die neu entstandene Datei hat denselben Namen wie die Originaldatei, die Dateiendung wird um die Endung `.p7s` erweitert. Beispiel: Der Dateiname von `beispiel.docx` wird zu `beispiel.docx.p7s`. Die enthaltene Originaldatei kann nur durch eine geeignete Verifikationsanwendung eingesehen oder extrahiert werden, beispielsweise durch die Funktion "Verifizieren" des Governikus Signer.
- **Signatur als gesonderte Datei beifügen** (detached): Die Datei wird gemäß CAdES-Standard elektronisch signiert. Dabei entstehen zwei Dateien. Eine Datei ist die originale Eingangsdatei, die andere Datei enthält die elektronische Signatur gemäß CAdES (detached). Für den Nachweis von Integrität und Authentizität werden beide Dateien benötigt. Wird beispielsweise die Datei `beispiel.docx` mit dieser Option elektronisch signiert, entsteht die Datei mit der elektronischen Signatur `beispiel.p7s`. Ist das Zielverzeichnis das Originalverzeichnis, wird die `.p7s` Datei dort abgelegt. Haben Sie ein neues Zielverzeichnis gewählt, so werden Originaldatei und `.p7s`-Datei dort abgelegt. Sollen Integrität und Authentizität in diesem Fall verifiziert werden, müssen beispielsweise der Funktion "Verifizieren" des Governikus Signer beide Dateien übergeben werden.

Signieren von PDF-Dokumenten (PAdES)

- **Standardsignaturformat verwenden**: PDF-Dateien werden, wie alle anderen Dateien, in dem Format signiert, das unter **Standardsignaturformat (CAdES)** ausgewählt ist, siehe oben.
- **PDF-Signatur erstellen**: Wenn Sie diese Option wählen, erreichen Sie die sonst ausgegrauten Felder "Signaturfeld-Vorlage" und "Grund der Unterschrift". Bei diesem Format wird die Signatur innerhalb der PDF-Datei abgelegt. Eine so signierte PDF-Datei hat die Endung `_signed.pdf`.
  - **Signaturfeld-Vorlage**: Wenn Sie bereits Vorlagen erstellt oder importiert haben, können Sie hier eine Vorlage auswählen. Wenn Sie die Option "Keine" wählen, wird die PDF-Signatur mit den Einstellungen vorgenommen, die im Dialogfenster "Einstellungen" in der Registerkarte "PDF" gespeichert sind. Sie erreichen die Registerkarte "PDF" über den Link "Signatureinstellungen" rechts über der Auswahlliste. Die Registerkarte "PDF" ist im Kapitel 6.3.1 erklärt.
  - **Grund der Unterschrift**: Hier können Sie den Grund Ihrer Unterzeichnung (z. B. "sachlich richtig" oder "zur Zahlung freigegeben") eintragen. Es können maximal 50 Zeichen eingegeben werden. Wenn Sie keinen Grund angeben möchten, lassen Sie dieses Eingabefeld einfach leer.



Hinweis: Wenn Sie hier einen Grund der Unterschrift eingeben und auf der Registerkarte "PDF" ist die Option "Unsichtbares Signaturfeld" ausgewählt, wird der Grund nicht in der signierten PDF-Datei sichtbar.

Signieren von XML-Dokumenten (XAdES)

XAdES ist ein Akronym für XML Advanced Electronic Signatures. Wählen Sie hier, wie verfahren werden soll, wenn das zu signierende Dokument ein XML-Dokument ist.

- **Standardsignaturformat verwenden**: Es wird nicht versucht, eine Signatur im XAdES-Format zu erstellen. In diesem Fall wird die Signatur der XML-Datei in einer eigenen Datei mit der zusätzlichen Dateiendung `.p7s` abgelegt (CAdES detached).

- **XML-Signatur erstellen**: Für das Signieren von XML-Dateien müssen zwei Fälle unterschieden werden:
  - **Strukturinformation vorhanden**: In diesem Fall wird versucht, eine Signatur im XAdES-Format anzubringen. Dies funktioniert nur, wenn die Strukturinformation (Style-Sheet) der XML-Datei im XML-Viewer hinterlegt wurde. Ein Vorteil dieses Formats ist, dass die Gültigkeit von Dokumenten die so signiert werden vergleichsweise lang ist, unabhängig von verwendeten Verschlüsselungs-algorithmen. Das XML-Fachformat ist im Kapitel 6 beschrieben. Wird ein Fachformat erkannt, gibt dieses entweder vor, dass ein bestimmter Teil der XML-Datei signiert wird oder die gesamte Datei. Es kann auch vorgegeben sein, dass die Signatur im Format "XAdES detached" erzeugt wird.
  - **Keine XML-Strukturinformation**: Dies ist der Standardfall. Die Signatur der XML-Datei wird in einer eigenen Datei hinterlegt (CAdES detached). Die Signatur wird in einer zweiten Datei mit der zusätzlichen Dateiendung `.sig` abgelegt.

	**Hinweis**: Wenn eine XML-Signatur erstellt werden soll, wird das zu signierende Dokument immer einer Prüfung auf Standard-konformität und Darstellbarkeit unterzogen (vgl. Kapitel 8, Abschnitt Bewertete sichere Anzeige). Werden diese Kriterien nicht erfüllt, kann keine XML-Signatur erstellt werden.

	**Achtung**: Die Option "XML-Signatur erstellen" führt bei der Benutzung von Signaturkarten oder Softwarezertifikaten mit einem ECC-Schlüssel zum Abbruch des Signaturvorgangs. Die vom Governikus Signer benutzte Java-Standard-Bibliothek unterstützt derzeit keine XML-Signaturen mit ECC-Schlüsseln. Von dieser Einschränkung sind die folgenden Signaturkarten betroffen: • PKS-ECC-Signaturkarte Version 2.0 der TeleSec und • Neuer Personalausweis.

Zeitstempel Server

- **Externen Zeitstempel anbringen**: Sie haben die Möglichkeit, das Anbringen von externen Zeitstempeln zu aktivieren. Wenn Sie diese Option auswählen, wird der Link "Zeitstempeleinstellungen" aktiv, der zum Einstellungsdialog führt. Dieser Dialog ist im Kapitel "6.3" erklärt.

Das Anfordern und Anbringen von Zeitstempeln ist nur im Rahmen der Signaturerstellung möglich. Im Dialog Signieren können Sie auf der Dialogseite Optionen entscheiden, ob Sie der elektronisch signierten Datei einen externen Zeitstempel hinzufügen wollen. Sie können die Checkbox auswählen:

- **Ja**: Wenn Sie Ihrer elektronischen Signatur einen externen Zeitstempel hinzufügen wollen, muss ein Zeitstempelserver konfiguriert sein. Die Konfiguration erreichen Sie über den Link "Zeitstempelserver festlegen" am rechten Rand dieses Dialogabschnitts. Über diesen Link wird der Dialog Einstellungen mit der Registerkarte Zeitstempel aufgerufen, der im vorausgegangenen Kapitel erklärt ist. Unabhängig vom gewählten Signaturformat (siehe Dialogabschnitt oben) wird damit zu jeder erstellten Signaturdatei ein elektronisch signierter Zeitstempel angefordert, der in einer eigenen Datei zurückgeliefert wird. Diese Datei hat das Suffix `.tsp`. Fordern Sie beispielsweise für die Signatur der Datei `beispiel.doc` einen externen Zeitstempel an, so hat die

Datei mit dem Zeitstempel den Namen `beispiel.doc.p7s.tsp` (für Signaturformat CAdES detached und enveloped). Diese Datei lässt sich nur zusammen mit der Signaturdatei (`beispiel.doc.p7s`) verifizieren. Signieren Sie beispielsweise die Datei `beispiel.pdf` im Format PAdES (siehe oben), erhalten Sie die Datei `beispiel_signed.pdf` und die zugehörige Zeitstempeldatei `beispiel_signed.pdf.tsp`.

- **Nein**: Wenn Sie keinen externen Zeitstempel anbringen möchten.

6.3 Einstellungen

Der Dialog "Einstellungen" wird in einem eigenen Fenster angezeigt. Sie erreichen den Dialog entweder über den Link "Signatureinstellungen" im Dialogabschnitt "Signieren von PDF-Dokumenten" oder über den Link "Zeitstempeleinstellungen" im Dialogabschnitt "Zeitstempel Server". Beachten Sie, dass die o. g. Dialogabschnitte nicht vorhanden sein können. In diesem Fall kann der Dialog "Einstellungen" nicht geöffnet werden und die Einstellungen werden vollständig durch Ihren Dienstanbieter vorgegeben.

Ausgegraute oder ausgeblendete Dialogseiten

Bitte beachten Sie, dass Dialogseiten ganz oder teilweise ausgegraut sein können oder gar nicht angezeigt werden, wenn die dort vorhandenen Einstellungen bereits von Ihrem Diensteanbieter festgelegt wurden.

Registerkarten

Der Dialog kann vier Registerkarten enthalten. Es können allerdings auch eine oder mehrere Registerkarten ausgeblendet sein. Im Folgenden werden die Registerkarten und die dort vorhandenen Einstellungsmöglichkeiten erklärt.

Buttons auf allen Registerkarten

Auf allen Registerkarten finden Sie diese Buttons:

- **Hilfe**: Dieser Button ruft die Online-Hilfe auf.
- **Vorübergehend übernehmen**: Mit diesem Button speichern Sie die gewählten Einstellungen. Bitte beachten Sie, dass Ihre Konfiguration nur für diesen Aufruf der WebEdition gespeichert wird. Wenn Sie die WebEdition schließen, wird Ihre Konfiguration verworfen.
- **Abbrechen**: Mit diesem Button verlassen Sie den Dialog, ohne dass Ihre Einstellungen gespeichert werden.

6.3.1 Registerkarte PDF

Die Einstellungen, die Sie hier vornehmen können, werden nur wirksam, wenn Sie bei der Funktion Signieren auf der Dialogseite "Optionen" die Einstellung "PDF-Signatur erstellen" ausgewählt haben. PDF-Dokumente bieten die Möglichkeit, zusätzlich zur eigentlichen Signatur sicht- und druckbare Signaturinformationen im Dokument aufzunehmen. Die

Registerkarte PDF ist in mehrere Dialogabschnitte unterteilt, die im Folgenden erklärt werden.

Signaturfeld anlegen

- **Kein sichtbares Signaturfeld**: Wenn Sie diese Option wählen, wird kein sichtbares Signaturfeld angelegt. Die Signatur wird nur in der PDF-Datei im Bereich "Unterschriften" angezeigt.
- **Sichtbares Signaturfeld**: Es wird ein sichtbares Signaturfeld angelegt, dessen Erscheinungsbild Sie in den folgenden Dialogabschnitten festlegen können.
- **Art**: Hier wählen Sie aus, ob die Darstellung Text (zusätzliche Unterschriftsinformationen), eine Grafik oder beides enthalten soll.
- **Layout**: Wenn Sie im Feld "Art" die Option "Text und Grafik" ausgewählt haben, können Sie hier auswählen, wie Grafik und Text zueinander angeordnet werden sollen.
- **Vorlage**: Über den Button Vorlage können Sie Einstellungen für die PDF-Signatur als Vorlagen verwalten. Dies ist im folgenden Kapitel erklärt.

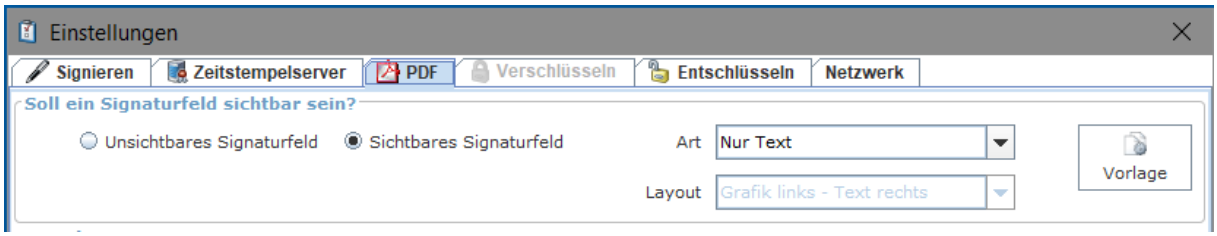


Abbildung 11: Dialogabschnitt "Soll ein Signaturfeld sichtbar sein?"

6.3.1.1 Vorlagen verwalten

Nachdem Sie auf der Registerkarte "PDF" Einstellungen vorgenommen haben, können Sie diese Einstellungen als Vorlage speichern. Eine Vorlage fasst Einstellungen für eine PDF-Signatur zusammen, damit Sie eine bestimmte Konfiguration einfach und schnell abrufen können. Alle hier erstellten Vorlagen stehen beim Signieren auf der Dialogseite "Optionen" zur Auswahl zur Verfügung. Über den Button "Vorlage" wird eine Auswahlliste aufgeklappt, auf der Sie diese Möglichkeiten haben:

- **Liste der Vorlagennamen**: Als erstes in der Auswahlliste werden alle vorhandenen Vorlagen aufgelistet. Wenn Sie auf den Namen einer Vorlage klicken, werden die Einstellungen auf der Registerkarte "PDF" so umgestellt, wie Sie es in der Vorlage festgelegt haben.
- **Speichern**: Wenn Sie den Eintrag "Speichern" wählen, wird ein neues Dialogfenster angezeigt. In diesem Dialog können Sie einen Namen für die Einstellungen eingeben, die Sie als Vorlage speichern wollen, siehe nächste Abbildung. Klicken Sie nach der Eingabe eines Vorlagenamens auf den Button OK. Der Name ist danach in der Liste der Vorlagennamen auswählbar. **Hinweis**: Wählen Sie einen möglichst sprechenden Namen für eine Vorlage, damit daraus die dahinterstehende Konfiguration klar wird.

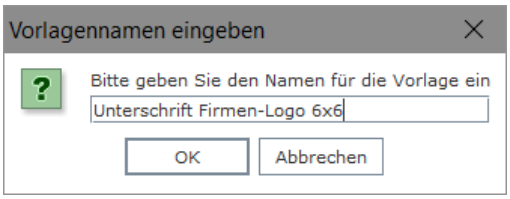


Abbildung 12: Vorlagennamen eingeben

- **Verwalten**: Wenn Sie den Eintrag "Verwalten" wählen, wird ein neues Dialogfenster geöffnet, über das Sie Vorlagen löschen, importieren und exportieren können.
  - **Löschen**: Wenn Sie eine Vorlage löschen wollen, klicken Sie die Vorlage in der Liste an und klicken Sie dann auf Löschen. Es wird eine Sicherheitsabfrage angezeigt, die Sie bestätigen müssen.
  - **Importieren**: Sie können Vorlagen, die zuvor mit dem Governikus Signer erstellt und exportiert wurden, über diesen Button importieren. Der Button öffnet einen Dateiauswahldialog. Wählen Die das Verzeichnis aus, in dem sich eine Vorlagendatei befindet. Eine Vorlage hat die Dateiendung `.signpdf_tmpl`. Nach dem Import steht die Vorlage zum Signieren von PDF-Dateien zur Verfügung.
  - **Exportieren**: Sie können Vorlagen exportieren, beispielsweise um sie anderen Benutzern des Governikus Signer zur Verfügung zu stellen.

	**Achtung**: Beim Speichern einer Vorlage mit Grafik wird nur der Pfad zur Grafik und deren Dateiname gespeichert. Wenn Sie eine Vorlage mit Grafik exportieren, um sie für andere Personen zur Verfügung zu stellen, speichern Sie die Grafik auf einem Server, der für alle verfügbar ist.

Abbildung 13: Vorlagen verwalten mit Beispielvorlagen

6.3.1.2 Visualisierung

Zusätzliche Unterschriftsinformationen

In diesem Abschnitt können Sie zusätzliche Informationen zu Ihren sichtbaren Signaturen eintragen. Diese Angaben werden innerhalb des PDF-Dokumentes im sichtbaren Signaturfeld angelegt und können mit einem geeigneten Anzeigeprogramm (z. B: Adobe Reader) angesehen werden.

- **Unterzeichner:** Wählen Sie hier, wie Ihre persönlichen Daten angezeigt werden:
  - **Aus Signaturzertifikat entnehmen**: Wenn Sie diese Option wählen, wird bei jeder Signatur der Name aus dem Signaturzertifikat verwendet.

  - **Name**: Wenn Sie diese Option wählen, können Sie einen abweichenden Namen (z. B. mit abgekürztem Vornamen) mit maximal 50 Zeichen eintragen oder, wenn Sie keinen Unterzeichner angeben möchten, das Feld leer lassen.

- **Ort:** Hier können Sie den Ort der Unterzeichnung mit einer Länge von maximal 50 Zeichen eintragen oder, wenn Sie keinen Ort angeben möchten, das Feld leer lassen.
- **Datum:** Wenn Sie die Checkbox auswählen, wird das aktuelle Datum als zusätzliche Information in der Visualisierung dargestellt. Bitte beachten Sie, dass in der Signatur selbst der Signaturzeitpunkt immer enthalten ist.
- **Formatierung**: Unter "Formatierung" können Sie die Darstellungsform des Datums verändern.

Zu den zusätzlichen Unterschriftsinformationen gehört auch der Unterschriftsgrund. Da hier aber eine häufigere Änderung zu erwarten ist, erfolgt die Eingabe des Grundes direkt im Dialog "Signieren" im Schritt "Optionen".

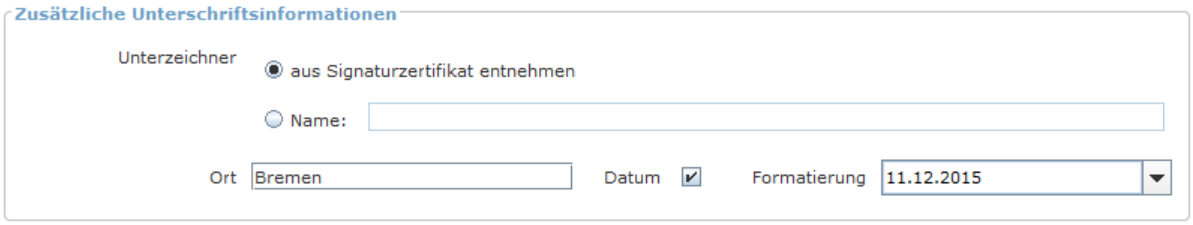


Abbildung 14: Dialogabschnitt "Zusätzliche Unterschriftsinformationen"

6.3.1.3 Signaturfeld platzieren

Ein Signaturfeld erstellen, falls dieses nicht vorhanden ist

Entscheiden Sie in diesem Dialogabschnitt als erstes über diese Option:

- **Nicht ausgewählt**: Wenn diese Option **nicht** ausgewählt ist, sind diese Fälle zu unterscheiden:
  - In dem PDF-Dokument, das signiert werden soll, wurden bereits vorher ein oder mehrere sichtbare Signaturfelder angelegt. In diesem Fall werden die auf der Registerkarte "PDF" konfigurierten Texte und Grafiken in eines der Felder eingefügt. Wenn nur ein sichtbares Signaturfeld enthalten ist, wird dieses beim Signieren automatisch benutzt. Wenn mehrere sichtbare Signaturfelder vorhanden sind, werden Sie beim Signieren dazu aufgefordert, eines der Felder auszuwählen.
  - In dem PDF-Dokument, das signiert werden soll, sind bereits sichtbare Signaturfelder angelegt worden, die allerdings bereits sichtbare Signaturen enthalten. In diesem Fall wird eine unsichtbare Signatur eingefügt.
  - In dem PDF-Dokument, das signiert werden soll, wurde kein sichtbares Signaturfeld angelegt. In diesem Fall wird eine unsichtbare Signatur eingefügt.
- **Ausgewählt**: Wenn diese Option ausgewählt ist, wird ein sichtbares Signaturfeld erstellt, wenn noch kein anderes sichtbares Signaturfeld vorher erstellt wurde oder alle sichtbaren Signaturfelder bereits belegt sind.

In den folgenden Feldern können Sie einstellen, wie und wo das sichtbare Signaturfeld erstellt wird. Sie müssen dazu die Gesamtgröße in Form eines Rechtecks sowie, wenn Sie sowohl Grafik als auch Text einfügen möchten, das Größenverhältnis von Grafik zu Text vorgeben. Die Große der ausgewählten Grafik wird automatisch an den so zur Verfügung gestellten Platz angepasst, wobei die Seitenverhältnisse gleichbleiben. Die Beispiele in der

folgenden Abbildung veranschaulichen dies. Details zu den Einstellungsmöglichkeiten werden nachfolgend beschrieben.

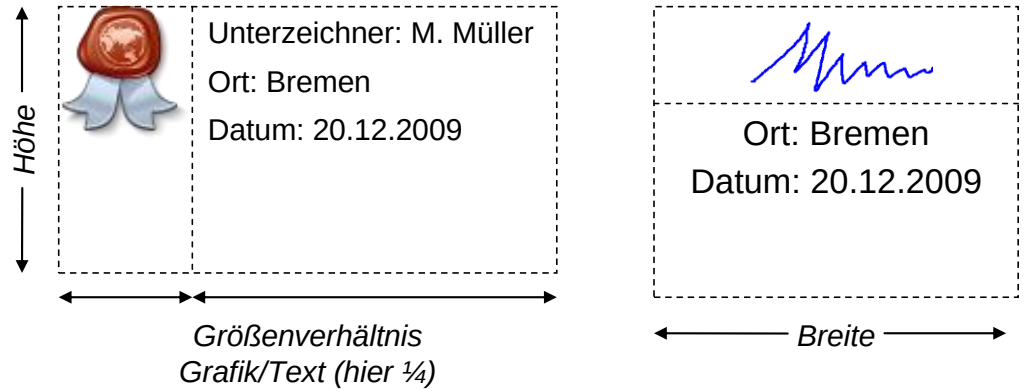


Abbildung 15: Beispiele für eine Visualisierung mit Grafik und Text

In der Abbildung oben dienen die gestrichelten Linien nur der Veranschaulichung. Der Dialog bietet folgende Einstellungen:

- **Seite:** Wählen Sie hier aus, ob die Darstellung auf der ersten oder auf der letzten Seite des Dokumentes erfolgen soll.
- **Grafik/Text:** Bestimmen Sie hier, wie groß die Grafik im Verhältnis zum Text sein soll. Die Gesamtgröße ergibt sich aus den über "Breite" bzw. "Höhe" definierten Maßen. Haben Sie unter "Anordnung" bestimmt, dass Text und Grafik nebeneinanderliegen, wird die Aufteilung horizontal vorgenommen, ansonsten vertikal.
- **Höhe:** Bestimmen Sie hier, welche Höhe die sichtbaren Signaturinformationen überdecken sollen.
- **Breite:** Bestimmen Sie hier, welche Breite die sichtbaren Signaturinformationen überdecken sollen.
- **Position:** Legen Sie fest, an welcher Position auf der Dokumentenseite die sichtbaren Signaturinformationen dargestellt werden sollen. Halten Sie dazu den roten Rahmen mit der Maus fest und ziehen Sie ihn an die Position, an der die Visualisierung auf der Seite angezeigt werden soll.

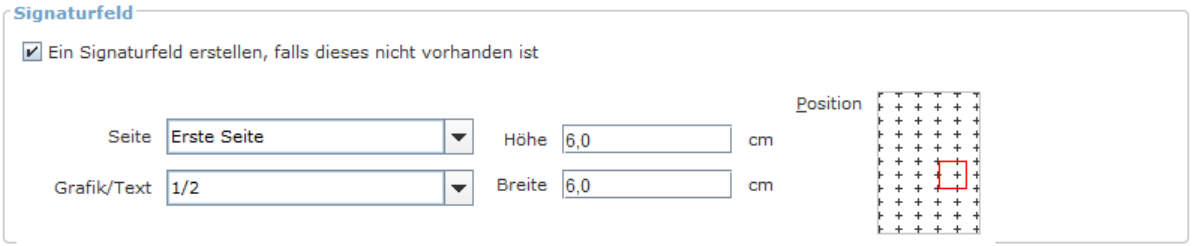


Abbildung 16: Dialogabschnitt "Signaturfeld platzieren"

6.3.1.4 Schrift

Hier können Sie Details zu der Textdarstellung einstellen.

- **Kompatibilität**: Soll die PDF/A Kompatibilität des PDF-Dokuments auch mit einer sichtbaren Signatur erhalten bleiben, wählen Sie bitte diese Option aus. Damit ist die individuelle Auswahl von Schriftart und Schriftfarbe nicht mehr möglich.

- **Schriftart**: Da die Darstellung des Dokuments auf unterschiedlichen Systemen möglich sein muss, ist die Auswahl der Schriftarten auf die Standardschriftarten "Times New Roman", "Helvetica" und "Courier New" beschränkt.
- **Schriftfarbe**: Wählen Sie aus der Drop-down-Liste die Schriftfarbe aus.
- **Schriftgröße automatisch verkleinern**: Ist die Checkbox neben "Schriftgröße" aktiviert, wird die Schriftgröße automatisch verkleinert, sofern der Text nicht in den definierten Platz passt (s. o.).
- **Schriftgröße**: Wählen Sie hier die Schriftgröße aus der Drop-down-Liste.
- **Formatierung**: Wählen Sie aus der Drop-down-Liste die Ausrichtung der Schrift aus.

6.3.1.5 Grafik

Legen Sie fest, welche Grafik eingefügt werden soll. Sie können eine Grafik aus der Drop-down-Liste auswählen oder eine andere Grafik über einen Dateiauswahldialog laden. Die Grafik muss im Format PNG, JPG oder GIF vorliegen und sollte keine transparenten Bereiche enthalten. Die ausgewählte Grafik wird in einer Vorschau dargestellt.

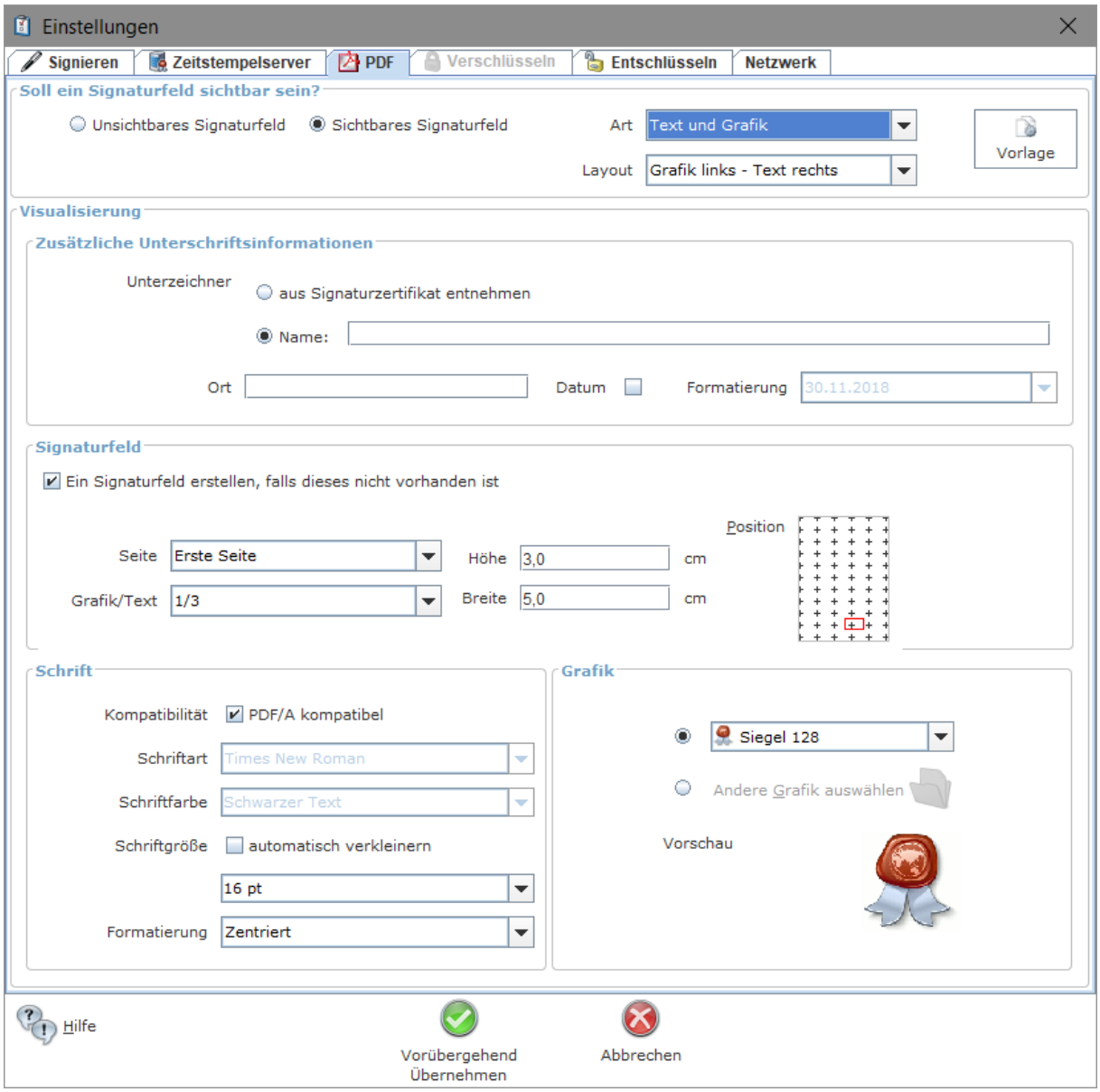


Abbildung 17: Registerkarte PDF im Dialog "Einstellungen"

6.3.2 Registerkarte Signieren

Auf dieser Registerkarte finden Sie die folgenden Einstellungen:

Anzahl der einzusehenden Dateien

Nach Signaturgesetz (SigG) § 17 muss eine Software, mit der Dateien elektronisch signiert werden können, die Möglichkeit bieten, die Dateien vor dem Signieren anzuschauen.

- **Einsehen erforderlich**: Wenn Sie hier die Checkbox auswählen, können Sie im nächsten Feld eine Prozentzahl angeben.
- **Mindestanzahl**: Diese Zahl gibt den Anteil der Dateien in Prozent vor, die Sie anschauen müssen, bevor die WebEdition mit dem Anbringen der elektronischen Signatur beginnen kann. Das Signieren wird erst freigegeben, wenn die entsprechende Anzahl angezeigt wurde. Um sicherzugehen, sollten Sie hier 100 angeben. Wenn dies in Ihren Arbeitsabläufen nicht praktikabel ist und Sie der Korrektheit der von Ihnen zusammengestellten Dateien in der Dateiliste vertrauen, können Sie hier eine Zahl zwischen 1 und 100 angeben.

Sichere Anzeige

- **Sichere Anzeige auch für Originaldateien verwenden**: Wählen Sie diese Option, wenn Sie die sichere Anzeige für Dateien im Dateiauswahl Dialog verwenden möchten (erster Dialog der Funktion "Signieren"). Wenn Sie diese Option nicht auswählen, wird das Programm zur Anzeige der Datei benutzt, dass auf Ihrem Rechner mit dem entsprechenden Dateityp assoziiert ist.

Quelldateien löschen

Hier können Sie auswählen, ob die von Ihnen zum Signieren ausgewählten Dateien nach erfolgreicher Erstellung signierter Dateien gelöscht werden sollen. Dies gilt für folgende Signaturformate:

- PAdES (PDF-Inline)
- CAdES (PKCS#7) enveloping
- CAdES (PKCS#7) detached (nur wenn ein separates Zielverzeichnis verwendet wird)
- XAdES enveloped

Die Quell-Dateien werden erst nach dem erfolgreichen Signieren gelöscht. **Hinweis**: Die Dateien werden endgültig gelöscht. Es existieren danach nur noch die signierten Dateien. Die folgende Abbildung zeigt die Registerkarte "Signieren" im Dialog Einstellungen.

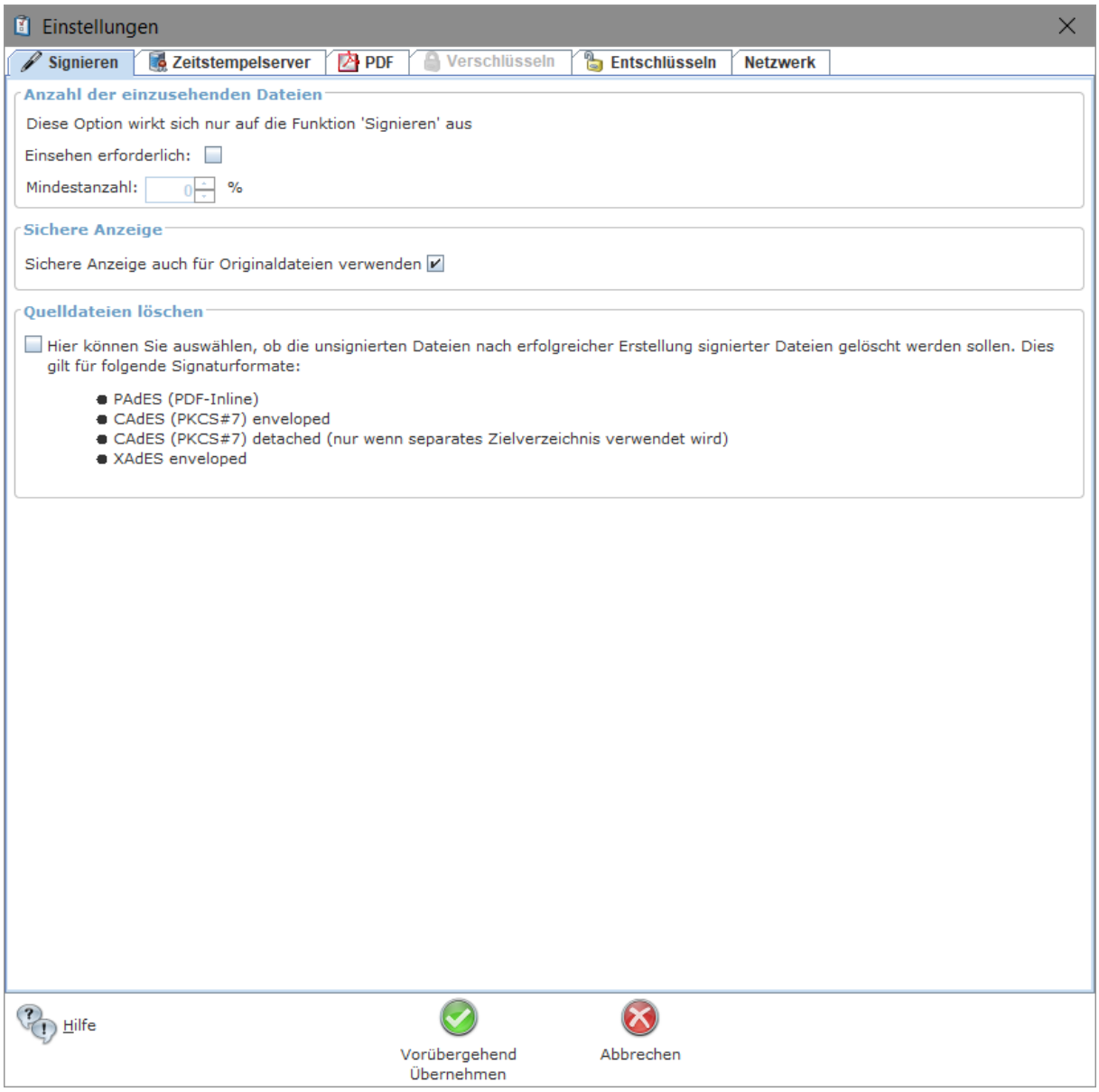


Abbildung 18: Registerkarte Signieren

6.3.3 Registerkarte Zeitstempelserver

Hier können Sie eine Verbindung zum Zeitstempelserver eines Governikus Servers konfigurieren. Die Verbindungsdaten zum Governikus Server erfragen Sie bitte bei Ihrem Governikus Betreiber. Füllen Sie die Felder wie folgt aus:

- **Servername**: Geben Sie hier den Namen oder die IP-Adresse des Governikus Servers an, beispielsweise `www.example.com` oder `127.0.0.1`.
- **Port**: Geben Sie hier die Nummer des Ports an, über den die Kommunikation mit dem Governikus Server durchgeführt wird. Für gewöhnlich ist dies Port 80.
- **Pfad**: Der Pfad bezieht sich auf die genaue Adresse auf dem Governikus Server. Er fängt mit einem Schrägstrich an, beispielsweise:
  - `/gov2core/services/Gov2CoreService`
- **OperationID**: Der hier benötigte Wert wird Ihnen vom Governikus Betreiber zugewiesen. Die OperationID weist den Governikus Server an, bestimmte Instruktionen

auszuführen. In diesem Fall wird eine Systemzeit zurückgeliefert oder eine signierte Zeit von einem Zeitstempeldienstanbieter, wenn dies vom Governikus Betreiber so eingestellt wurde. Der Wert ist beispielsweise `internalTimeStamp001`.

- **SystemID**: Der hier benötigte Wert wird Ihnen vom Governikus Betreiber zugewiesen. Die SystemID wird vom Governikus Betreiber eingerichtet, um bestimmte Dienste des Governikus Servers einer ausgewählten Gruppe von Anwendern zuzuweisen. Der Wert ist beispielsweise `systemid19923`.

Die nächste Abbildung zeigt die Registerkarte Zeitstempelserver.

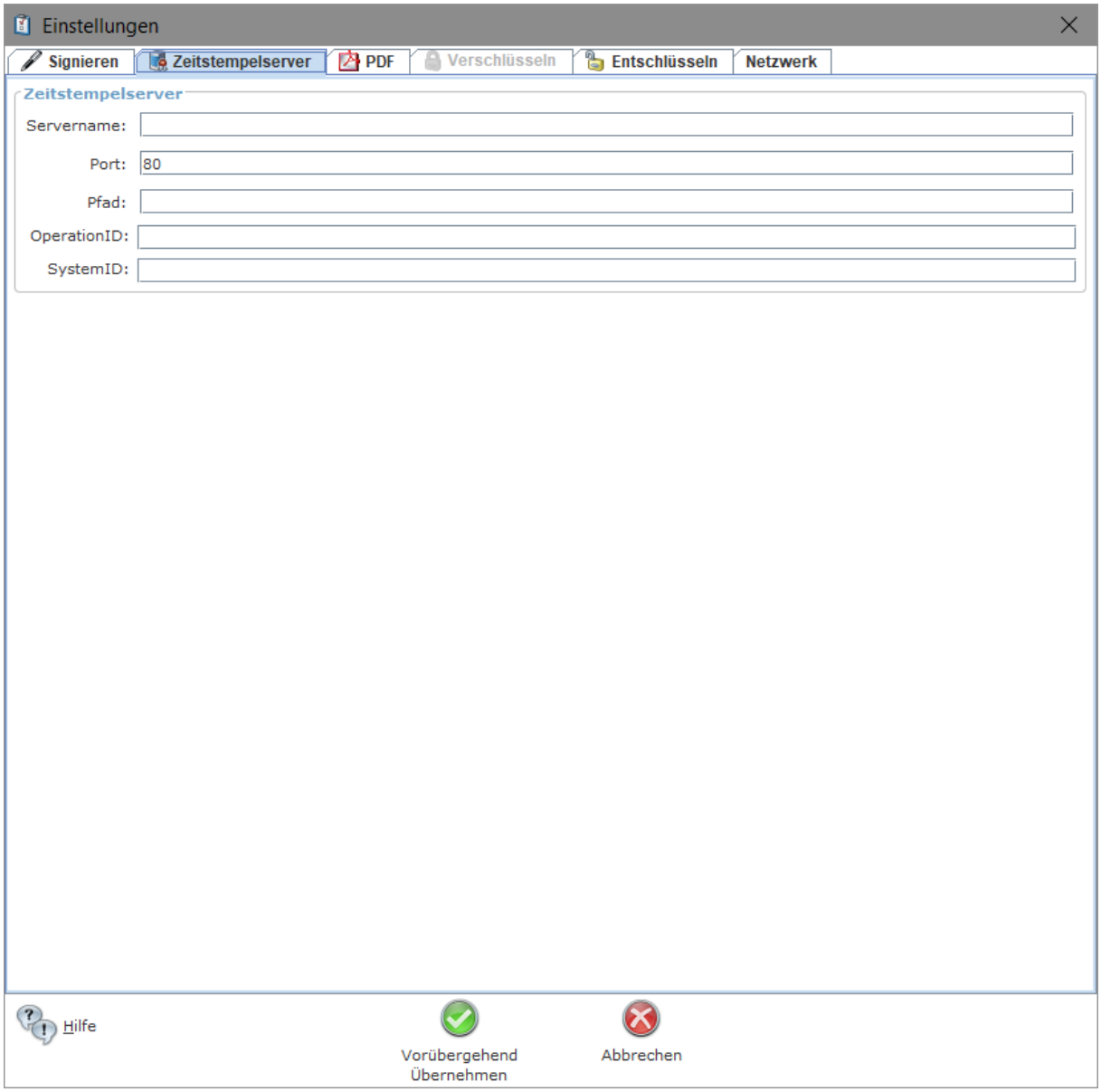


Abbildung 19: Registerkarte Zeitstempelserver

6.3.4 Registerkarte Netzwerk

Auf dieser Seite können einen Proxy-Server konfigurieren.

Proxy-Server

Wenn ein Proxy-Server zwischen Ihrem Rechner und dem Internet steht, müssen Sie hier die Zugangsdaten angeben. Ist bereits ein Proxy-Server auf Ihrem Computer eingestellt, wird automatisch dessen IP-Adresse hier angegeben. Andernfalls erhalten Sie die Daten für die Konfiguration des Proxy-Servers von Ihrem Administrator:

- **Servername**: Geben Sie hier den Namen oder die IP-Adresse des Proxy-Servers an, beispielsweise `www.example.com` oder `192.0.32.10`.
- **Port**: Geben Sie hier die Nummer des Ports an, über den die Kommunikation mit dem Proxy-Server durchgeführt wird. Für gewöhnlich ist dies Port 80.
- **Login/Passwort**: Proxy-Server verlangen normalerweise eine Authentifizierung. Geben Sie hier Login und Passwort an. Bitte beachten Sie, dass zwischen Groß- und Kleinschreibung unterschieden wird.
- **Ausnahmen**: Sie können hier Ausnahmen eintragen. Eine Ausnahme ist die Adresse eines Rechners, der im selben Netzwerk steht, wie Ihr Arbeitsplatzrechner und daher nicht über den hier angegebenen Proxy-Server zu erreichen ist. Fragen Sie Ihren Administrator, welche Ausnahmen hier eingetragen werden müssen.

Systemeinstellungen laden

Wenn der Button "Systemeinstellungen laden" aktiviert ist, können Sie über diesen Button die IP-Adresse und die Portnummer des Proxy-Servers automatisch laden, wenn auf Ihrem Rechner diese Einstellungen hinterlegt sind. Nach dem Laden dieser Einstellungen können Sie die Einträge weiterhin editieren.

Systemeinstellungen laden - Sonderfall PAC-Datei

PAC steht für Proxy-Auto-Configuration. Dies ist eine Datei, die von einem Administrator erstellt wird und systemweit in Ihrer Firma gilt. Sie enthält alle Proxy-Einstellungen, die für alle Rechner im Firmennetz gelten. Wenn Sie auf den Button Systemeinstellungen klicken und die Adresse zu einer PAC-Datei ist auf Ihrem Rechner eingestellt, werden die Einstellungen aus dieser Datei als Proxy-Einstellungen übernommen. Wenn eine PAC-Datei gefunden wird, können Sie keine Änderungen im Dialog vornehmen. Die Felder sind ausgegraut. Wenn eine PAC-Datei gefunden wurde, werden die Werte nicht im Dialog angezeigt.

Die folgende Abbildung zeigt die Konfiguration eines Proxy-Servers mit Beispieldaten.

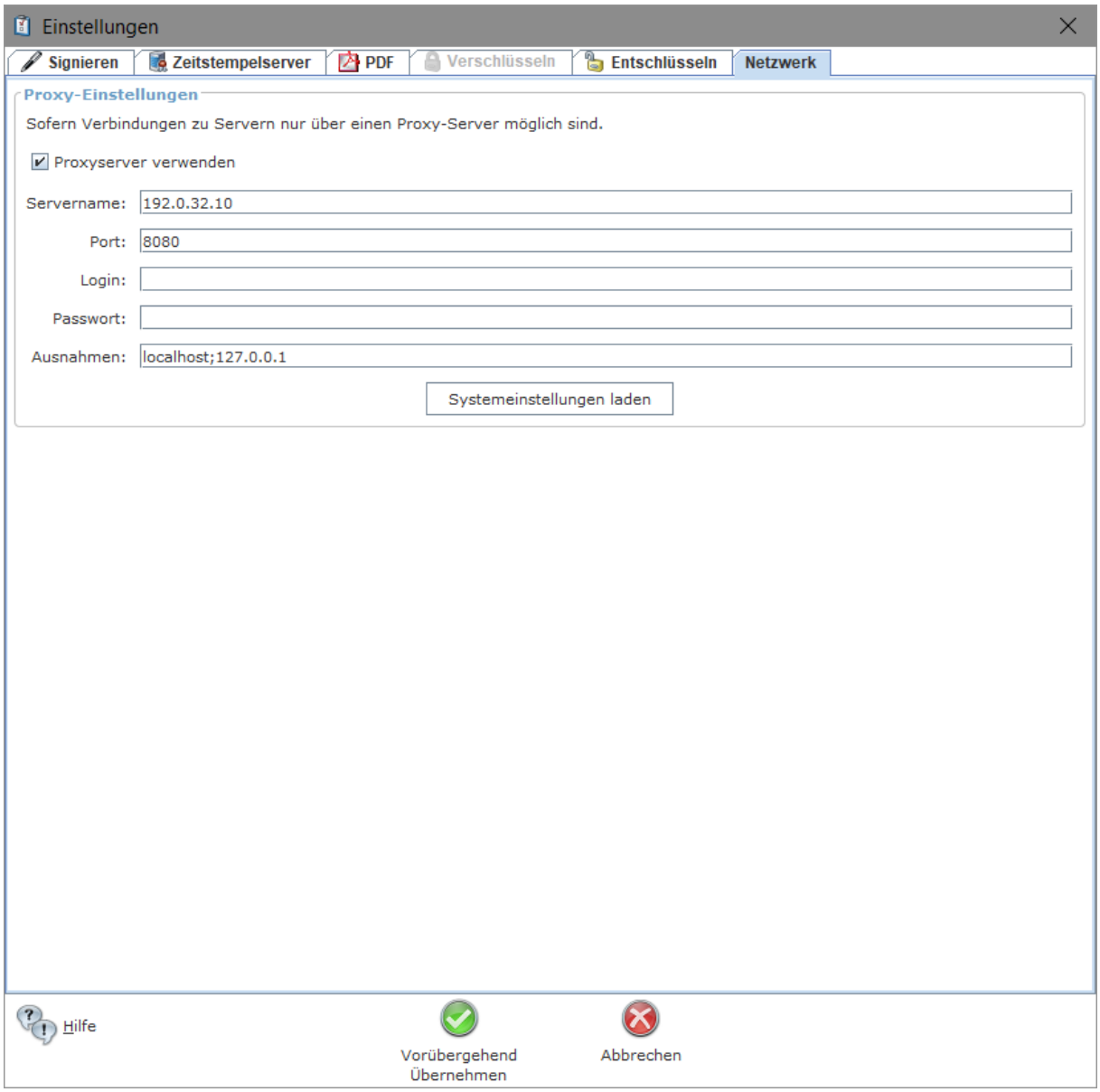


Abbildung 20: Registerkarte Netzwerk

6.4 Schlüssel wählen

Dialog ausgegraut

Dieser Dialog kann vollständig ausgegraut sein. In diesem Fall können Sie keine Auswahl treffen. Es wird Ihnen angezeigt, welche Option ausgewählt ist. Es wird in diesem Fall entweder vorausgesetzt, dass Sie Ihren Kartenleser angeschlossen und Ihre Signaturkarte eingelegt haben. In diesem Fall können Sie so vorgehen, wie im Kapitel "Signieren" erklärt. Oder Ihr Dienstanbieter hat bereits ein Softwarezertifikat (Schlüssel aus Datei) ausgewählt. In diesem Fall müssen Sie nach dem Start der WebEdition die PIN eingeben und danach so vorgehen, wie im Kapitel "Signieren" erklärt.

Möglich ist, dass nur die Option "Schlüssel aus Datei laden" ausgegraut ist. In diesem Fall wird nur ein Kartenleser angezeigt, wenn Sie diesen angeschlossen haben und eine Signaturkarte eingelegt haben. Wenn Sie Ihren Kartenleser nachträglich anschließen und dieser dann nicht angezeigt wird, schließen Sie die WebEdition mit dem Kreuzsymbol unten rechts und starten Sie die WebEdition erneut.

Auf dieser Dialogseite können Sie wählen, mit welchem Signaturschlüssel Sie Dateien elektronisch signieren wollen.

Signaturniveau

In diesem Dialogabschnitt können Sie vorgeben, mit welchem Signaturniveau Sie die Dateien signieren wollen. Die folgende Auswahl steht zur Verfügung:

- **Alle**: Mit dieser Auswahl bestehen keine Einschränkungen, es können auch Schlüssel genutzt werden, die ursprünglich zur Authentisierung oder Verschlüsselung erstellt wurden.
- **Qualifiziert**: Mit dieser Auswahl wird die Möglichkeit ausgegraut, Softwareschlüssel aus dem Dateisystem auszuwählen. Sie müssen einen Schlüssel von einer Signaturkarte oder dem neuen Personalausweis auswählen, die in einem angeschlossenen Kartenleser zur Verfügung steht. Bitte beachten Sie, dass qualifizierte Signaturen der eigenhändigen Unterschrift rechtlich gleichgestellt sind. Im Feld Schlüsselauswahl werden nur Schlüssel angezeigt, die für eine qualifizierte Signatur geeignet sind.
- **Fortgeschritten**: Mit dieser Auswahl können Sie Softwareschlüssel vom Dateisystem auswählen. Zudem können Sie auch Schlüssel von einer Signaturkarte auswählen. Dabei werden allerdings im Dialogabschnitt "Schlüsselauswahl" nur die Schlüssel von der Signaturkarte angezeigt, die **nicht** für qualifizierte Signaturen geeignet sind.

Dialog aktiv

In diesem Dialogabschnitt können Sie durch Anklicken auswählen, mit welchem Signaturschlüssel Sie Dateien elektronisch signieren wollen. Der ausgewählte Speicherort wird blau umrandet.

-  **Schlüssel aus Datei laden**: Diese Auswahl kann ausgegraut sein: Wenn Sie einen Schlüssel aus einer Datei laden wollen, klicken Sie auf dieses Symbol und navigieren Sie an die Stelle im Dateisystem, an der dieser Schlüssel abgelegt ist. Es muss ein Keystore geladen werden, dessen Dateiname mit dem Suffix `.p12` oder `.pfx` endet. Ein Keystore enthält ein Softwarezertifikat und das benötigte Schlüsselpaar für die asymmetrische Verschlüsselung. Bitte beachten Sie, dass bei Softwarezertifikaten die Authentizität des Signierenden nur dann nachgewiesen werden kann, wenn ein Trust Center das Softwarezertifikat ausgegeben hat und Sie für die Ausstellung Ihres Softwarezertifikats Ihre Identifikationsunterlagen vorgelegt haben. Beim Laden der Keystore-Datei werden Sie nach der PIN für den Keystore gefragt.
-  **Signaturkarte**: Diese Auswahl wird nur angezeigt, wenn Sie einen Kartenleser angeschlossen haben. Sie ist nur dann auswählbar, wenn Sie eine Signaturkarte eingelegt haben. Unter diesem Symbol steht der Name des Kartenlesers, der von der WebEdition erkannt wurde. Mit einer Signaturkarte können Sie in der Regel qualifizierte, elektronische Signaturen oder qualifizierte, elektronische Signaturen mit Anbieterakkreditierung erstellen.

	**Hinweis**: Der Diensteanbieter hat die Möglichkeit, Signaturkarten abzulehnen, die nur auf ein **Pseudonym** ausgestellt sind, beispielsweise nur auf einen Künstlernamen. In diesem Fall sind die Schlüssel nicht auswählbar. Benutzen Sie eine Signaturkarte die auf Ihren Namen ausgestellt ist.

Wichtiger Hinweis

Achtung:

- **Kartenleser vom Rechner trennen**: Trennen Sie **niemals** einen Kartenleser vom Rechner, solange das Programm ausgeführt wird. Beenden Sie das Programm, bevor Sie einen Kartenleser vom Rechner trennen.
- **Entfernen der Signaturkarte**: Entfernen Sie **niemals** während des Signaturvorgangs die Signaturkarte aus dem Kartenleser. Warten Sie damit, bis das Programm den Signaturvorgang beendet hat.

Signieren mit kontaktlosen Signaturkarten

Wenn Sie eine Signaturkarte verwenden, auf die kontaktlos zugegriffen wird, und einen entsprechenden Kartenleser verwenden, müssen Sie auch hier vor der Schlüsselauswahl zunächst die Zugangsnummer eingeben. Der Ablauf ist identisch zu der Signatur mit dem Personalausweis. Die sechsstellige Zugangsnummer ist ebenfalls auf der Signaturkarte aufgedruckt.

Signaturkarte erneut einlesen

Achtung: Lesen Sie unbedingt diesen Abschnitt, wenn die Signaturkarte nicht mehr gelesen werden kann!

Wird eine Signaturkarte während des Betriebs der WebEdition von der Signaturanwendungskomponente eines anderen Herstellers verwendet, kann es passieren, dass die WebEdition die Signaturkarte nicht mehr lesen kann, weil die andere Signaturanwendungskomponente diese nicht freigibt.

Wenn Sie die Signaturkarte wieder mit der WebEdition benutzen wollen, verfahren Sie wie folgt:

- Beenden Sie unbedingt die Signaturanwendungskomponente des anderen Herstellers.
- Nehmen Sie die Signaturkarte aus dem Kartenleser und stecken Sie sie gleich wieder in den Kartenleser zurück, oder
- Klicken Sie auf den Button "Karten neu einlesen" unten links auf der Dialogseite "Schlüssel wählen".

Die Signaturkarte wird erneut eingelesen und Sie können danach wieder Schlüssel von der Karte auswählen. Der Kartenleser, in dem die Signaturkarte steckt, ist von dieser Aktion nicht betroffen und arbeitet weiter wie zuvor.

Abgelaufene Zertifikate

Wenn Sie eine Signaturkarte oder einen Keystore auswählen, die nur Zertifikate enthalten, deren Gültigkeit bereits abgelaufen ist, können Sie keines dieser Zertifikate auswählen. Signaturen können nur mit Zertifikaten erstellt werden, die zum Zeitpunkt der Erstellung der Signatur gültig sind.

Sonderfall: Wenn Sie eine Signaturkarte oder einen Keystore auswählen, die zum Teil gültige und zum Teil ungültige Zertifikate enthalten, können Sie jedes dieser Zertifikate auswählen. Wenn Sie hier allerdings ein ungültiges Zertifikat auswählen, wird dieses beim Signieren zurückgewiesen.

Schlüsselauswahl

Wenn Sie einen Speicherort ausgewählt haben, werden in diesem Dialogabschnitt die verfügbaren Schlüssel angezeigt. In einem Keystore oder auf einer Signaturkarte können mehrere Schlüssel enthalten sein. Wenn dies so ist, müssen Sie genau einen Schlüssel durch Anklicken in der Liste auswählen. Der ausgewählte Schlüssel wird blau umrandet.

Zertifikat anzeigen

Zum ausgewählten Schlüssel gehört ein Zertifikat, das Sie über das Lupensymbol anzeigen können. Sie können die Zertifikatsanzeige entweder mit dem OK-Button  beenden oder das Zertifikat mit dem Speichern-Button  als Datei abspeichern.

	**Hinweis**: Bitte beachten Sie, dass die hier getroffenen Einstellungen beim nächsten Programmaufruf der WebEdition nicht mehr vorhanden sind.

6.5 Zielverzeichnis wählen

Im Zielverzeichnis werden die Dateien abgelegt, nachdem Sie die Funktion Signieren ausgeführt haben.

Dialog ausgegraut

Dieser Dialog kann ausgegraut sein. In diesem Fall können Sie keine Auswahl treffen. Es wird Ihnen angezeigt, welche Option ausgewählt ist, also entweder das Quellverzeichnis, oder ein Zielverzeichnis. Wenn ein Zielverzeichnis ausgewählt wurde, wird der Ort des Verzeichnisses unter dem Button "Zielverzeichnis auswählen" angezeigt.

Dialog aktiv

Wenn der Dialog nicht ausgegraut ist, bietet er Ihnen zwei Optionen. Sie können entweder das Quellverzeichnis nutzen oder ein neues Zielverzeichnis auswählen. Die getroffene Auswahl wird blau umrandet.

Zielverzeichnis wählen

- **Quellverzeichnis nutzen**: Nachdem Sie die Funktionen Signieren ausgeführt haben, werden die Ergebnisdateien in dasselbe Verzeichnis geschrieben, aus dem die jeweilige Originaldatei stammt.
- **Zielverzeichnis wählen**: Klicken Sie auf diesen Button öffnet sich ein Auswahldialog, über den Sie ein Verzeichnis festlegen können, in das alle Ergebnisdateien geschrieben werden. Der Pfad zum Zielverzeichnis wird danach unter dem Button "Zielverzeichnis wählen" angezeigt.

Lokale Kopie erstellen

Wenn Sie eine Kopie der signierten Datei an einem zusätzlichen Ort speichern möchten, können Sie diesen hier auswählen.

- **Zielverzeichnis wählen**: Wählen Sie über den Button ein Verzeichnis aus, in dem Sie eine Kopie der signierten Datei speichern wollen.

	**Hinweis**: Bitte beachten Sie, dass die hier getroffenen Einstellungen beim nächsten Programmaufruf der WebEdition nicht mehr vorhanden sind.

6.6 Signieren

In der Liste werden alle Dateien aufgeführt, die Sie bei der Dateiauswahl ausgewählt haben, siehe Kapitel 6.1. Nachdem Sie auf den Signieren-Button am unteren Rand des Dialogfensters geklickt haben, werden nacheinander alle Dateien signiert, die in der Liste aufgeführt sind.

PIN-Eingabe

Wenn Sie mit einer Signaturkarte signieren, werden Sie bei jeder Datei, die signiert werden soll, zur Eingabe der PIN für das Signaturzertifikat aufgefordert.

	**Achtung**: • **Kartenleser vom Rechner trennen**: Trennen Sie **niemals** einen Kartenleser vom Rechner, solange das Programm ausgeführt wird. Beenden Sie das Programm, bevor Sie einen Kartenleser vom Rechner trennen. • **Entfernen der Signaturkarte**: Entfernen Sie **niemals** während des Signaturvorgangs die Signaturkarte aus dem Kartenleser. Warten Sie damit, bis das Programm den Signaturvorgang beendet hat.

Neue oder andere Signaturkarte

Wenn Sie eine Signaturkarte das erste Mal im Governikus Signer verwenden oder wenn Sie eine andere Signaturkarte verwenden, als die, die zuvor im Governikus Signer verwendet wurde, müssen Sie vor dem ersten Signieren einmalig auch die globale PIN eingeben.

Die globale PIN autorisiert die Benutzung der Schlüssel des Verschlüsselungszertifikats. Dies ist notwendig, da die Kommunikation zwischen Kartenleser und Governikus Signer aus Sicherheitsgründen nur verschlüsselt erfolgen darf. Es werden Verschlüsselungszertifikate zwischen dem Kartenleser und dem Governikus Signer ausgetauscht, die solange gültig bleiben, solange Sie zum Signieren dieselbe Signaturkarte benutzen. Wechseln Sie die Signaturkarte, müssen Sie einmalig vor dem Signieren die globale PIN dieser Signaturkarte angeben.

Mehrfaches Signieren einer Datei

Mit der WebEdition können Dateien auch mehrfach signiert werden, indem die WebEdition mit einer bereits signierten Datei erneut aufgerufen wird. Der Diensteanbieter kann jedoch unterbinden, dass eine bereits signierte Datei mit demselben Schlüssel erneut signiert wird. In diesem Fall wird ein Dialogfenster angezeigt, dass Sie entsprechend informiert, siehe nächste Abbildung.

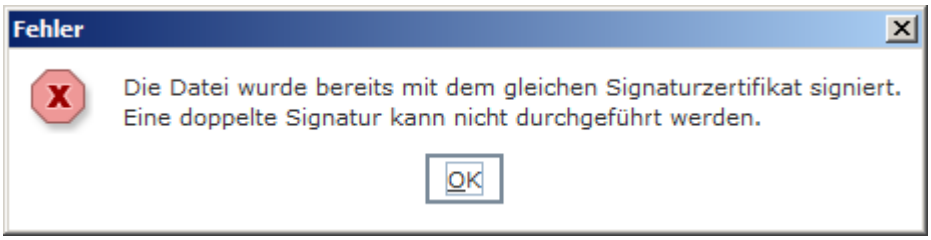


Abbildung 21: Warndialog bei doppelter Signatur

Nach der Anzeige dieses Dialogfensters wird die WebEdition geschlossen. Benutzen Sie beim nächsten Aufruf der WebEdition mit derselben Datei einen anderen Schlüssel für das Signieren.

Die Listendarstellung

Die Zeilen in der Listendarstellung haben die folgenden Spalten:

- **Datei**: Zeigt den Namen der zum Signieren ausgewählten Datei an. Wenn Sie den Mauszeiger über den Dateinamen legen, wird der vollständige Pfad angezeigt.
-  : Das Augensymbol wird angezeigt, wenn die Datei vor dem Signieren angezeigt wurde. Das Symbol ist grau, wenn die Datei noch nicht angezeigt wurde.
-  : Über das Lupensymbol wird die Dateianzeige aufgerufen; klicken Sie dazu auf das Symbol. Es wird dasjenige Programm für die Anzeige aufgerufen, das mit diesem Dateityp assoziiert ist, also beispielsweise das Programm "MS Word" für Dateien mit dem Suffix `.doc`. **Hinweis**: Lesen dazu bitte auch unbedingt den folgenden Abschnitt "Mindestanzahl einzusehender Dateien".
- **Status**: Diese Spalte zeigt den Verarbeitungsstatus der Datei an. Diese Meldungen sind möglich:
  - **Neu**: Die Datei wurde noch nicht verarbeitet;
  - **In Arbeit**: Die Verarbeitung wird gerade durchgeführt.
  - **Fehler**: Bei der Verarbeitung ist ein Fehler aufgetreten. Die Fehlerursache wird an die Fachanwendung weitergeleitet, über die Sie die WebEdition aufgerufen haben oder an den Dienstanbieter.
  - **Fertig**: Die Datei wurde erfolgreich signiert.
- **Ergebnisdatei**: Hier werden der Pfad und der Name der Ergebnisdatei angezeigt.

Mindestanzahl einzusehender Dateien

Wenn Sie mit dem Button "Signieren" den Signiervorgang auslösen, ist es möglich, dass ein Hinweisdialog angezeigt wird und der Signiervorgang blockiert ist. Der Hinweisdialog hat folgenden Text: "Die Mindestanzahl der einzusehenden Dateien wurde noch nicht erreicht. X% der Dateien müssen noch eingesehen werden." Die Angabe X% wird im konkreten Fall durch eine Zahl ersetzt, die den Anteil der einzusehenden Dateien vorgibt.

Wird dieser Hinweisdialog angezeigt, müssen die auf dieser Dialogseite aufgeführten Dateien erst von Ihnen angesehen werden, bevor der Signiervorgang ausgelöst wird. Benutzen Sie dazu bitte den Button mit dem Lupe-Symbol.

Das Ansehen der Dateien vor dem Signieren kann über die Einstellungen der WebEdition erzwungen werden und wird entweder vom Dienstanbieter eingestellt, oder dies wurde im Dialog Einstellungen von Ihnen so festgelegt, siehe Kapitel 6.3.2. Bitte verwenden Sie in diesem Fall ein vertrauenswürdiges Anzeigeprogramm, das Ihnen den Inhalt der gewählten Datei korrekt darstellt. Wenn Sie den Button "Anzeigen" benutzen (Lupe-Symbol), versucht

die WebEdition die Datei mit dem Programm zu öffnen, das auf Ihrem Rechner für diesen Dateityp als Standardanwendung eingetragen ist oder fordert Sie dazu auf, ein entsprechendes Programm auszuwählen.

Dieser Vorgang kann dem Signiervorgang vorangestellt sein, damit Sie sich vorher vom Inhalt der Datei überzeugen können, die Sie danach Signieren. Mit dem Auslösen der Anzeige wird im Hintergrund ein Sicherungsmechanismus ausgelöst, der überwacht, ob die Datei in der Zeit zwischen dem Ansehen und dem Signieren verändert wurde. Wurde die Datei in dieser Zeit verändert, wird ein entsprechender Warndialog angezeigt, der Sie auf diese Veränderung hinweist.

Dialogseite "Erweiterte PDF-Signatur"

Wenn Ihr Administrator dies eingestellt hat, kann vor dem Signieren einer PDF-Datei eine Dialogseite in einem neuen Fenster angezeigt werden. In diesem Fall verfahren Sie bitte so, wie im Kapitel 6.7" Erweiterte PDF-Signatur" beschrieben.

6.6.1 Dialogabschnitt unterhalb der Listendarstellung

Hier werden die folgenden Angaben angezeigt.

Signaturniveau

Dieses Feld kann die Werte unbekannt, fortgeschritten, qualifiziert oder qualifiziert mit Anbieterakkreditierung enthalten. Beachten Sie: Die WebEdition wird mit einer Liste ausgeliefert, die alle bekannten Aussteller von Zertifikaten enthält.

- **unbekannt**: Haben Sie ein Softwarezertifikat oder ein Zertifikat von einer Signaturkarte zum Signieren ausgewählt, dessen Aussteller nicht in der Liste der bekannten Aussteller enthalten ist, ist das Signaturniveau immer "unbekannt".
- **fortgeschritten**: Softwarezertifikate von bekannten Ausstellern und Zertifikate von Signaturkaten, die eigentlich zum Authentifizieren gedacht sind und deren Aussteller bekannt sind, haben das Signaturniveau "fortgeschritten".
- **qualifiziert und qualifiziert mit Anbieterakkreditierung**: Nur mit Signaturzertifikaten von Signaturkarten, deren Aussteller bekannt sind, können Signaturen erstellt werden, deren Signaturniveaus qualifiziert oder qualifiziert mit Anbieterakkreditierung sind. Nur diese Signaturen sind einer handschriftlichen Unterschrift rechtlich gleichgestellt.

Standardsignaturformat

Die Angaben in diesem Feld richten sich nach der Auswahl die auf der Dialogseite "Optionen" getroffen wurde.

- **CAdES Dokument in Signatur einbetten**: Signatur im Format "CAdES". Die Signatur und die signierten Daten werden gemeinsam ein einer neuen Datei hinterlegt. Der Name der neuen Datei erhält die zusätzliche Dateierweiterung `.p7s`.
- **CAdES Signatur als gesonderte Datei beifügen**: Signatur im Format "CAdES". Die Signatur wird in einer eigenen Datei hinterlegt, die den Dateinamen der signierten Datei trägt und die Dateierweiterung `.p7s`.

Signieren von PDF-Dokumenten

- **Standardsignaturformat (CAdES)**: Dieser Wert wird angezeigt, wenn auf der Dialogseite "Optionen" im Dialogabschnitt "Signieren von PDF-Dokumenten" die Einstellung "Standardsignaturformat verwenden" ausgewählt wurde.

Die weiteren Angaben, die hier angezeigt werden können, richten sich danach, welches Signaturformat für das Einbetten von PDF-Signaturen (PAdES) ausgewählt wurde. Das Akronym PAdES steht für **P**DF **Ad**vanced **E**lectronic **S**ignatures und bezeichnet den Standard TS 102 778, der vom European Telecommunications Standards Institute, kurz ETSI, verabschiedet wurde. Dieser Standard setzt auf den bekannten PDF-Signaturen auf, die in den Normen ISO 32000 und ISO 19905 definiert sind und das PDF-Signaturformat erweitert. PAdES ermöglicht die zukunftssichere Verifikation von signierten PDF-Dokumenten. PAdES entspricht den Anforderungen der EU an elektronische Signaturen. Diese Einstellung kann vom Diensteanbieter für PDF-Dateien auch bereits vorausgewählt sein.

- **PDF-Signatur (PAdES) - einfaches Signaturfeld**: Bei diesem Format wird die Signatur innerhalb der PDF-Datei abgelegt. Eine so signierte PDF-Datei hat die Endung `_signed.pdf`. Diese Angabe wird auch angezeigt, wenn eine Vorlage ausgewählt wurde, mit der ein sichtbares Signaturfeld benutzt werden soll. Die Erstellung von Vorlagen für PDF-Dateien ist in Kapitel 6.3.1 erklärt.

Sonderfall PDF-Datei mit sichtbaren Signaturfeldern

Wenn Sie eine PDF-Datei mit sichtbaren Signaturfeldern signieren, in der mehr als ein freies sichtbares Signaturfeld enthalten ist, **müssen** Sie ein Signaturfeld auswählen.

- **Auswählen**: Blättern Sie zum Auswählen im Dialogfenster mit der PDF-Datei auf die Seite, auf der das Signaturfeld angelegt wurde, und wählen Sie es durch Anklicken aus. Sie können das Signaturfeld auch aus der Tabelle auswählen, die oben rechts im rechten Teil des Dialogfensters angezeigt wird.
- **Auswahl bestätigen**: Bestätigen Sie die Auswahl Ihres Signaturfeldes mit "Speichern". Der Dialog wird geschlossen und das Signieren wird fortgesetzt. Ihre sichtbare Signatur wird in dem Signaturfeld angebracht, das Sie soeben ausgewählt haben.

	**Hinweis**: Signaturfelder, die bereits eine Signatur enthalten, können nicht mehr ausgewählt werden.

	**Achtung**: Die Auswahl des Signaturfelds auf der Dialogseite ist erfolgreich, wenn ein dunkler Rahmen um das Signaturfeld angezeigt wird und in der Tabelle "Unterschriftsfelder", rechts oben, die Checkbox mit dem entsprechenden Signaturfeld ausgewählt ist. Andernfalls wird nach dem Speichern die Fehlermeldung angezeigt, dass das Signaturfeld nicht gefunden wurde.

Signieren von XML-Dokumenten

Die Anzeige ist abhängig davon, was Sie auf der Dialogseite "Optionen" im Dialogabschnitt "Signieren von XML-Dokumenten" ausgewählt haben:

- **Standardsignaturformat (CAdES)**: In diesem Fall wird die Signatur der XML-Datei als Standardsignatur erzeugt. Es entsteht eine Datei mit der Endung `.p7s`.
- **XML-Signatur (XAdES)**: In diesem Fall wird versucht, eine Signatur im XAdES-Format anzubringen. Dies funktioniert nur, wenn die Strukturinformation (Style-Sheet) der XML-Datei im XML-Viewer hinterlegt wurde. Ist die Strukturinformation vorhanden, wird eine Datei mit diesem Namen erzeugt `<Dateiname>_signed.xml`. Ist die Strukturinformation nicht vorhanden, wird eine Standardsignatur erzeugt.

Zeitstempel

Dieses Feld kann die Werte "Ja" und "Nein" haben. Wenn "Ja" angezeigt wird, wird der Signatur ein signierter Zeitstempel in einer eigenen Datei hinzugefügt, der bestätigt, dass die zu signierende Datei zum Zeitpunkt der Anbringung der Signatur existierte. Die folgende Abbildung zeigt die Dialogseite "Signieren" mit einer Beispielbelegung.

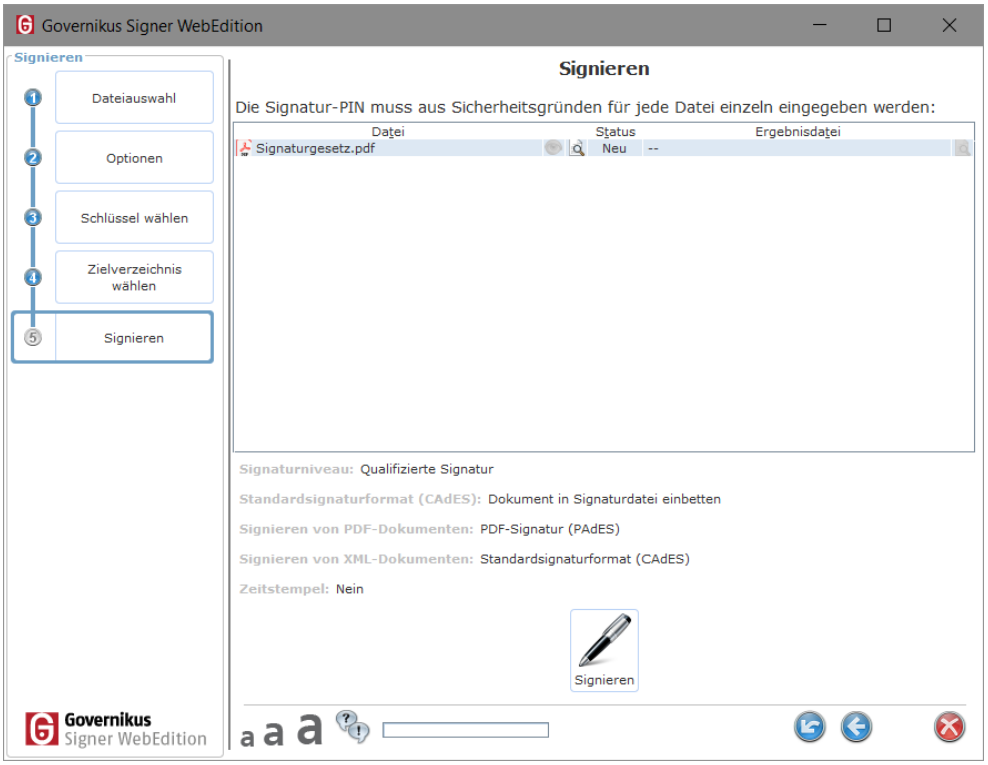


Abbildung 22: Dialogseite Signieren

Ergebnisdatei vorhanden

Wenn beim Erstellen der Ergebnisdatei bemerkt wird, dass eine Datei mit gleichem Namen im Zielverzeichnis und/oder im Verzeichnis für lokale Kopien bereits vorhanden ist, wird der Dialog "Zieldatei vorhanden" angezeigt. Sie haben hier die Möglichkeit, eine Auswahl zu treffen.

- **Überschreiben**: Die neue signierte Datei ersetzt die bereits vorhandene.
- **Umbenennen**: Beim Umbenennen wird der Datei das aktuelle Datum im Dateinamen vorangestellt.
- **Abbrechen**: Sie können die Verarbeitung auch abbrechen.

Sollten Sie mehrere Dateien signieren, besteht beim Überschreiben oder Umbenennen zusätzlich die Möglichkeit, diese Aktion auf alle nachfolgend zu signierenden Dateien anzuwenden, deren Ergebnisdateien ebenfalls bereits vorhanden sind. Wählen Sie dazu die Option "Aktion für nachfolgende Dateien automatisch durchführen" im selben Dialog.

Diese Option hat keine Auswirkung, wenn Sie "Abbrechen" wählen. In diesem Fall wird der Dialog bei jeder weiteren, bereits vorhandenen Ergebnisdatei erneut angezeigt. Wird die Verarbeitung abgebrochen, wird dies als Fehler gewertet.

Sonderfälle Stapelsignaturkarte und Multisignaturkarte

Stapelsignaturkarten sind besondere Signaturkarten, die das Signieren mehrerer Dateien (typisch sind 100 Signaturen) mit einmaliger PIN-Eingabe ermöglichen. Multisignaturkarten

sind besondere Signaturkarten für die "Massensignatur", die eine unbegrenzte Anzahl von Signaturen pro PIN-Eingabe ermöglichen.

Die WebEdition unterstützt diese Signaturkarten dahingehend, dass für jeden Signaturvorgang nur einmal die PIN eingegeben werden muss, sofern nicht die von der Signaturkarte gesetzte Grenze erreicht wird. Die maximale Anzahl der Signaturen pro PIN-Eingabe ist zusätzliche durch die WebEdition auf maximal 500 Signaturen begrenzt.

Fehler während es Signiervorgangs

Wenn während des Signierens einer Datei ein Fehler auftritt, wird dies in einem Dialogfenster angezeigt und der Status der zu signierenden Datei wird auf "Fehler" gesetzt. Wenn Sie mehrere Dateien signieren und beim Signieren einiger oder aller Dateien entsteht ein Fehler, wird dies am Ende der Verarbeitung in einem Dialog angezeigt, der die Anzahl der aufgetretenen Fehler auflistet. Wenn Sie diesen Dialog mit "OK" schließen, wird auch die WebEdition beendet.

Sie kehren zur Fachanwendung zurück, über die Sie die WebEdition aufgerufen haben. Oder es wird die Webseite angezeigt, die Ihr Dienstanbieter für diesen Fall vorgesehen hat, wenn Sie den Programmaufruf nicht über eine Fachanwendung gestartet haben.

Abschluss des Signiervorgangs

Wenn der Signierungsprozess ohne Fehler durchgeführt werden konnte, beendet sich die WebEdition automatisch. Traten ein oder mehrere Fehler auf, wird dies durch ein Dialogfenster angezeigt. Die WebEdition wird dann mit bestätigen dieses Dialoges beendet. Ihr Dienstanbieter kann festlegen, wie danach verfahren wird. Entweder kehren Sie zur aufrufenden Fachanwendung zurück oder Sie werde auf eine Seite weitergeleitet, die der Dienstanbieter festgelegt hat. Der Dienstanbieter kann auf so einer Seite beispielsweise die Statusmeldungen der WebEdition auflisten. So dass Sie Erfolgs- oder Fehlermeldungen erneut nachlesen können.

6.7 Erweiterte PDF-Signatur

Wenn Ihr Administrator dies eingestellt hat, kann vor dem Signieren einer PDF-Datei eine Dialogseite mit dieser PDF-Datei in einem neuen Fenster angezeigt werden. Auf dieser Dialogseite sollen Sie ein Signaturfeld auswählen, in das während des Signiervorgangs Ihre Signatur eingefügt wird. Es ist möglich, dass keine Signaturfelder in der PDF-Datei enthalten sind. In diesem Fall können Sie Signaturfelder anlegen.

6.7.1 Signaturfeld auswählen

Wenn das zu signierende Dokument bereits vorbereitete leere Signaturfelder enthält, blättern Sie im Dialogfenster in der PDF-Datei auf die Seite, auf der das Signaturfeld angelegt wurde, und wählen Sie es durch Anklicken aus. Sie können das Signaturfeld auch aus der Tabelle "Signaturfeldliste" auswählen, die oben rechts im rechten Teil des Dialogfensters angezeigt wird. Jedes der Signaturfelder kann genau eine PDF-Signatur aufnehmen. Wenn Sie das Signaturfeld ausgewählt haben, schließen Sie das Dialogfenster mit dem Button "Speichern/Übernehmen". Sie können danach auf der Dialogseite "Signieren" das Signieren fortsetzen.

6.7.2 Signaturfelder anlegen

Auf dieser Dialogseite können Sie Felder anlegen, die sichtbare Signaturen in PDF-Dokumenten aufnehmen können. Das Anlegen dieser Felder ist bei PDF-Dateien immer möglich. Im Folgenden wird der Aufbau und die Benutzung der Dialogseite erklärt.

Hinweis: Das Anlegen von Feldern für sichtbare PDF-Signaturen kann an mehreren Stellen erfolgen:

- Auf der Dialogseite "Dateiauswahl" über das Kontextmenü.
- Auf der Dialogseite "Signieren" über das Kontextmenu in der Dateiliste.
- Beim Auslösen des Signiervorgangs, wenn die Dialogseite angezeigt wird.

Mitte der Dialogseite

In der Mitte der Dialogseite wird der Inhalt der PDF-Datei angezeigt. Unter dieser Anzeige sind ein Feld, das die aktuelle Seitennummer anzeigt und die Anzahl der insgesamt vorhandenen Seiten. Darunter befinden sich die Buttons zum Umblättern, über die Sie die Seite auswählen können, auf der Sie Signaturfelder anlegen wollen.

Bestehende Signaturfelder werden in blau angezeigt, neu hinzugefügte Felder werden gelb angezeigt. Neu hinzugefügte Felder können mit der Maus verschoben und in der Größe verändert werden. Wie Sie Felder hinzufügen, ist im folgenden Absatz erläutert.

Linke Dialogseite

Hier können Sie bestimmen, wie viele Unterschriftsfelder angelegt werden sollen.

- **Feldeinstellungen** - oben links: Greifen Sie ein Feld mit der Maus und ziehen Sie es auf die von ihnen ausgewählte Seite der PDF-Datei.
  - Symbol "einzelnes Quadrat": Wenn Sie genau ein Signaturfeld einfügen wollen, ziehen Sie dieses Symbol auf die PDF-Seite.
  - Symbol "Quadrat mit vier Feldern": Wenn Sie mehrere Signaturfelder gleichzeitig einfügen wollen, ziehen Sie dazu dieses Symbol auf die PDF-Seite. Die Anzahl der mit diesem Symbol gleichzeitig erstellten Signaturfelder bestimmen Sie im darunterliegenden Abschnitt "Details" über die Felder "Spalten" und "Zeilen".
- Nachdem Sie per Drag-and-drop Signaturfelder eingefügt haben, können Sie beispielsweise umblättern und auf einer anderen Seite weitere Unterschriftsfelder hinzufügen.
- **Details** - unten links: Hier können Sie festlegen, wie die eingefügten Unterschriftsfelder aussehen sollen.
  - **Name**: Löschen Sie den Standardtext oder geben Sie den Unterschriftsfeldern einen Namen, der nach dem Signieren über dem Feld angezeigt wird. Wird kein Text angegeben, werden die Unterschriftsfelder oben links fortlaufend nummeriert. Wenn Sie hier einen Text angegeben, wird dieser in jedem Unterschriftsfeld oben links zusammen mit einer fortlaufenden Nummerierung angezeigt.
  - **Breite** und **Höhe**: Geben Sie hier die Breite und die Höhe in Millimetern an, die das Unterschriftsfeld erhalten soll, wenn Sie diese auf die PDF-Seite ziehen. Wenn Sie eine Tabelle mit Unterschriftsfeldern erstellen, erhält jedes einzelne Feld diese Größe.

- **Anzahl Felder** - unten links**:** Sie können mehrere Unterschriftsfelder auf einmal per Drag-and-drop auf eine PDF-Seite ziehen.
  - **Spalten** und **Zeilen**: Wenn Sie die Anzahl von Spalten und Zeilen größer als eins wählen, wird beim Ziehen auf die PDF-Seite eine entsprechend aufgebaute Tabelle mit Unterschriftsfeldern eingefügt.

Rechte Dialogseite

- **Unterschriftsfelder**: In dieser Tabelle werden alle angelegten Unterschriftsfelder in einer Tabelle aufgelistet. Die erste Spalte zeigt die ausgewählten Felder, die mit einem Mausklick ausgewählt werden können. Die zweite Spalte enthält die Namen der Unterschriftsfelder. Die dritte Spalte enthält die Seitennummer, auf der die Unterschriftsfelder angelegt wurden.
-  **Änderungen verwerfen**: Benutzen Sie diesen Button um alle neu angelegten Unterschriftsfelder auf allen Seiten zu löschen. Bereits gespeicherte Felder können nicht gelöscht werden.
-  **Speichern/Übernehmen**: Benutzen Sie diesen Button, um die angelegten Unterschriftsfelder in der PDF-Datei zu übernehmen. Dieser Button schließt die Dialogseite.
-  **Beenden**: Dieser Button schließt die Dialogseite, dabei gehen alle Änderungen verloren.

7 Sichere Anzeige

Mit der sicheren Anzeige können Sie zu signierende oder bereits signierte Text-Dateien und TIFF-Bilddateien einsehen. Lesen Sie vor dem Signieren oder verifizieren von TIFF-Dateien das Kapitel 7.3 "Sichere TIFF-Anzeige", damit Sie potenziell unsichere Dateien untersuchen können. Auch in Text-Dateien können Zeichen enthalten, über die sich keine sichere Aussage treffen lässt. Lesen Sie dazu bitte das Kapitel 7.2 "Sichere Text-Anzeige".

Bei signierten Dateien können Sie darüber hinaus die Signaturzertifikate einsehen. Dieses und der grundsätzliche Umgang mit der sicheren Anzeige sind in den folgenden Kapiteln beschrieben.

Bitte beachten Sie, dass die sichere Anzeige ggf. von Ihrem Dienstanbieter nicht zur Verfügung gestellt wird.

7.1 Dateien anzeigen

Mit dem  Button können sowohl die noch zu bearbeitenden Dateien als auch die Ergebnisdateien (Ausnahme: Verschlüsseln) eingesehen werden.

Die sichere Anzeige wird automatisch für Dateien mit den Endungen `.p7s` `.txt`, `.tif` und `.tiff` sowie `.pdf` aufgerufen. Die sichere Anzeige für PDF-Dateien ist wichtig, da bei einem PDF-Dokument die Signatur im PDF-Dokument enthalten sein kann, je nach Einstellung beim Signieren.

Überwachung von Dateien beim Signieren

Wenn Sie im Governikus Signer Dateien zum Signieren auswählen und diese in der Dialogseite "Dateiauswahl" über den  Button anzeigen lassen, werden diese Dateien vom diesem Zeitpunkt an vom Governikus Signer überwacht. Es ist dabei unerheblich, ob die Dateien von der sicheren Anzeige oder von dem Programm angezeigt werden, das mit der Dateiendung assoziiert ist. Wird eine Datei, die auf der Dialogseite "Dateiauswahl" angezeigt wurde, zwischen dem Zeitpunkt der Anzeige und dem Zeitpunkt des Signierens verändert, wird diese Veränderung vom Governikus Signer durch einen Warndialog angezeigt. Damit ist sichergestellt, dass Sie nur die Dateien signieren, die zuvor angezeigt wurden und seitdem unverändert geblieben sind.

Aufbau des Dialogs

Der Anzeigedialog hat diesen Aufbau:

- **Menü "Datei"**: Oben rechts befindet sich eine Menüleiste, die das Menü "Datei" enthält. Darüber können Sie die sichere Anzeige beenden.

In einem Rahmen darunter folgen die Angaben zur Datei: Name, Pfad, Größe und Signaturformat. Darunter ist der Anzeigedialog wie folgt aufgeteilt.

Linke Seite des Dialogfensters - oben

Bei nicht signierten Dateien steht hier einfach der Dateiname. Bei signierten Dateien werden die Zusammenhänge von Signatur und signiertem Inhalt als Baumstruktur dargestellt. Die Struktur hängt auch vom Signaturformat ab, d.h. ob die Signatur in dem signierten Dokument enthalten ist (bei PDF-Dateien: PAdES), ob der signierte Inhalt in der Signaturdatei enthalten ist (CAdES enveloped) oder Signatur und signierter Inhalt in separaten Dateien vorliegen (CAdES detached).

Bei einer einfachen Signatur werden hier untereinander diese Einträge angezeigt:

- **Dateiname:** Die Baumstruktur beginnt immer mit dem Namen der der geöffneten (Signatur-) Datei. Wenn Sie diesen Eintrag auswählen, werden auf der rechten Seite Informationen zur Datei sowie Informationen zu der Signatur angezeigt.
- **Signatur**: Wenn Sie diesen Eintrag auswählen wird auf der rechten Seite der im Zertifikat hinterlegte Name, der Zeitpunkt der Anbringung der Signatur und der für den Hashwert benutzte Algorithmus inkl. Gültigkeitsende angezeigt. Zudem wird in der Zeile Integrität das Ergebnis der mathematischen Signaturprüfung angezeigt. Wird ein grüner Kreis mit weißen Haken angezeigt, ist das Dokument seit Anbringung der Signatur nicht verändert worden.

	**Hinweis**: Eine Validierung, d.h. ein Prüfung, ob das Zertifikat des Signierenden gültig und nicht gesperrt ist, findet nicht statt.

- **Signaturzertifikat**: Dieser Unterpunkt zu dem Eintrag "Signatur" enthält den Namen des Signaturinhabers. Wenn Sie diesen Eintrag auswählen, werden rechts die wichtigsten Zertifikatsinformationen angezeigt. Über die Schaltfläche "Speichern unter" können Sie das Zertifikat speichern.
- **Signierter Inhalt**: Der Eintrag ist abhängig vom Dateityp. Alle Dateitypen können mit dem "Speichern unter"-Button gespeichert oder entweder mit der sicheren Anzeige oder mit dem Programm, das mit der Dateiendung verbunden ist, angezeigt werden (siehe nächster Abschnitt "Linke Seite des Dialogfensters - unten"):
  - Ist die signierte Datei vom Typ `.txt` wird der Inhalt der Datei angezeigt, siehe hierzu Kapitel 7.2.
  - Ist Datei vom Typ .tif oder `.tiff` wird das TIFF-Bild angezeigt, siehe hierzu Kapitel 7.3.
  - Bei allen anderen Dateitypen wird Dateiname und -Endung angezeigt. Auf der rechten Seite steht, dass für dieses Dokument keine sichere Anzeige zur Verfügung steht.

Enthält das Dokument mehrere Signaturen, bzw. enthält die signierte Inhaltsdatei selber auch noch eine Signatur, werden über eine baumartige Darstellung die Zusammenhänge der Signaturen zum jeweilig signierten Dokument dargestellt.

Linke Seite des Dialogfensters - unten

Hier finden Sie diese Buttons:

-  **Anzeigen**: Wenn Sie eine signierte Datei in der sicheren Anzeige aufgerufen haben, markieren Sie auf der linken Seite die Zeile "Signierter Inhalt". Das Dokument wird Ihnen dann mit dem Programm angezeigt, dass auf Ihrem Computer mit dem entsprechenden Dateityp verbunden ist.

- **Speichern unter**: Unsignierte Dateien können Sie mit dieser Funktion erneut speichern, beispielsweise unter einem anderen Namen oder in einem anderen Verzeichnis. Bei signierten Dateien können Sie im linken Teil des Dialogfensters wählen, was Sie speichern möchten.
  - **Name der signierten Datei**: Wählen Sie den Namen der signierten Datei auswählen, können Sie diese erneut speichern, beispielsweise unter einem anderen Namen oder in einem anderen Verzeichnis.
  - **Name der Signatur**: Wenn Sie die Signatur auswählen, können Sie das Zertifikat speichern.
  - **Signierter Inhalt**: Wenn Sie den signierten Inhalt auswählen, können Sie die Datei ohne Signatur in ihrem ursprünglichen Format speichern, damit Sie diese dann mit dem auf ihrem Computer dafür vorgesehenen Programm öffnen können.

Hinweise zu PDF-Dokumenten

PDF-Dokumente werden grundsätzlich auch mit der sicheren Anzeige geöffnet, um Informationen zu einer ggf. enthaltenen Signatur darstellen zu können. Das Anzeigen des Dokumenteninhalts muss allerdings immer mit einer externen Anwendung erfolgen. Markieren Sie dazu den Dateinamen und wählen Sie anschließend unten links den "Anzeigen"-Button. Das PDF-Dokument wird mit dem Programm geöffnet und angezeigt, da auf Ihrem Rechner mit der Dateiendung `.pdf` verbunden ist.

Signierte PDF-Dokumente enthalten zu jeder Signatur eine zugehörige Dokumentenrevision, d.h. den Stand des Dokumentes, der jeweils signiert wurde. Diese Revisionen werden in der Baumstruktur dargestellt. Das Einsehen dieser Revisionen ist jedoch nicht aus der sicheren Anzeige heraus möglich.

7.2 Sichere Text-Anzeige

Die sichere Anzeige kann Text-Dateien im UTF-8-Format eindeutig anzeigen. Enthält die Datei potenziell nicht darstellbare Inhalte, ist keine eindeutige Anzeige möglich. In diesem Fall wird im Dialogfenster ein Warnhinweis angezeigt, dass eine vertrauenswürdige Anzeige nicht möglich ist (siehe Abbildung 23). Nicht eindeutig darstellbar sind z.B. Textdateien, die nicht dem UTF-8-Format entsprechen. Aber auch UTF-8-konforme Dateien können nicht darstellbare Zeichen enthalten, welche einen versteckten Inhalt darstellen könnten. Auch solche Dateien können nicht vertrauenswürdig angezeigt werden.

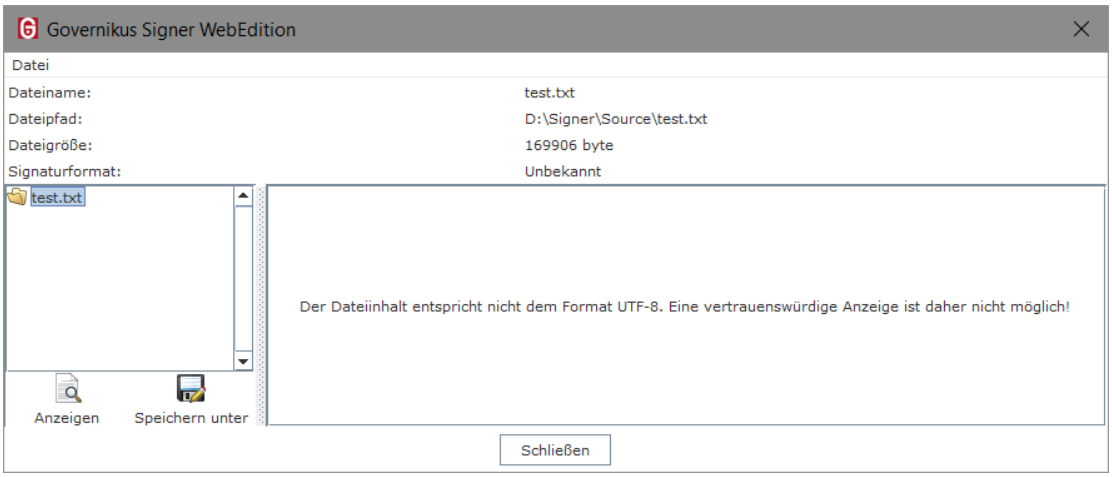


Abbildung 23: Warnhinweis bei nicht darstellbaren Zeichen

7.3 Sichere TIFF-Anzeige

Was ist TIFF

TIFF steht für **T**agged **I**mage **F**ile **F**ormat und beschreibt eine Basisstruktur für die Repräsentation von Bilddaten. Die Freiheitsgrade bei der Spezifikation des Aufbaus von Bilddaten im TIFF-Format haben dazu geführt, dass es TIFF in vielen verschiedenen Varianten gibt. Neu- oder weiterentwickelte TIFF-Formate können bei ADOBE Inc. angemeldet und veröffentlicht werden. TIFF ist heute ein weit verbreitetes Bildformat, dessen gängigste Ausprägungen von der überwiegenden Anzahl der Bildanzeigeprogramme dargestellt werden können.

Hinweis: Die TIFF-Spezifikation (Adobe TIFF™ Revision 6.0). ist erhältlich unter www.adobe.com. Darin sind u. a. ausführlich Aufbau und Inhalt von TIFF-Dateien beschrieben.

Die Komplexität der TIFF-Spezifikation ermöglicht die Darstellung von nahezu verlustfreien Bildern und Inhalten. Diese Komplexität bietet jedoch auch verschiedene Möglichkeiten, verdeckte oder aktive Inhalte in die Darstellung zu integrieren.

Der im Governikus Signer enthaltene Trusted TIFF-Viewer bietet Funktionen, um Inhalte, die angezeigt werden sollen, eindeutig darzustellen. Dem Anwender wird so versichert, dass die angezeigte Datei frei von verdeckten oder aktiven Inhalten ist. Befinden sich aktive oder nicht darstellbare Inhalte in einem Dokument, wird dies über entsprechende Hinweismeldungen dem Nutzer bekannt gegeben.

Die sichere TIFF-Anzeige verfügt über eine eigene Navigation. Hierüber können alle Bild- und Zusatzinformationen angezeigt werden. Weitere Funktionen ermöglichen gezielte Farbwertveränderungen, um potenzielle Manipulationsversuche auszuschließen.

Die Identifikation der TIFF-Bilder erfolgt anhand der Endung der Datei. Erlaubt sind hierbei `.tif` und `.tiff`. Nachfolgend werden alle unterstützten TIFF-Formate aufgeführt. Bei den unterstützten Kompressionsformaten werden nur Formate aufgelistet, die zum entsprechenden Farbformat passen. Beispielsweise reduziert bei Erstellung eines Farbbildes eine CCITT-Komprimierung das Bild auf schwarz-weiß. Formate, die in den folgenden Punkten nicht aufgeführt sind, werden nicht unterstützt.

Unterstützte Farbformate (PhotometricInterpretation)

- WhiteIsZero
- BlackIsZero
- RGB
- RGB Palette

Unterstützte Kompressionsformate (Compression)

- CCITT Group 3 1-dimensional modified Huffmann run length encoding (CCITT 1D)
- CCITT.4 bi-level encoding (Group 3 FAX 1D/2D)
- CCITT.6 bi-level encoding (Group 4 FAX)
- LZW
- PackBits
- Unkomprimiert

Unterstützte Farbtiefen (BitsPerSample)

Schwarz-Weiß-Bilder

In diesem Format wird nur 1 Bit pro Bildpixel unterstützt.

Graustufenbilder

In diesem Format werden nur 4 oder 8 Bit pro Bildpixel unterstützt.

Farbbilder

Es werden nur TIFF-Bilder im RGB-Farbraum unterstützt. Die RGB-Farben müssen direkt oder über eine Colormap gesetzt sein. Eine Farbinformation (Rot, Grün, Blau) eines Pixels darf maximal je 8 Bit groß sein, da bei feineren Abstufungen das korrekte Anzeigen des Bildes nicht sichergestellt werden kann. Bei den 16-Bit-Angaben in Farbpaletten erfolgt eine Prüfung, ob Kontraste vorhanden sind, die nicht in TrueColor darstellbar sind.

7.3.1 Aufbau und Struktur der sicheren TIFF-Anzeige

Beim Öffnen eines TIFF-Dokuments wird dieses, sofern sicher darstellbar, in einem eigenen Viewer innerhalb des Verwaltungsbereichs des Governikus Signer angezeigt.

	**Hinweis**: Bitte beachten Sie, dass bei geöffneten CAdES-Dateien der Verwaltungsbereich in zwei Abschnitte unterteilt ist. Der obere Bereich enthält die gewohnten Informationen zum Dokument, während der untere Bereich der sicheren TIFF-Anzeige vorbehalten ist.

Die sichere TIFF-Anzeige ist in folgende Bereiche unterteilt, siehe auch Abbildung 24.

Navigationsbereich (inklusive Vorschauanzeige)

Dieser Bereich (links in der Anzeige) beinhaltet eine Art Inhaltsverzeichnis zum Bild selbst. Neben dem Dokumentnamen auf der höchsten Ebene sind darunter alle vorhandenen Bilder des TIFF-Dokuments aufgeführt. Mit Öffnen der sicheren Anzeige ist standardmäßig immer das erste, gefundene Bild eines TIFF-Dokuments vor ausgewählt. Durch Wechsel der Gliederungspunkte kann zwischen den verschiedenen Bildern, sowie den Bild- und Zusatzinformationen hin und her gewechselt werden. Die Bild- und Zusatzinformationen sind einsehbar durch das Anklicken des Dateinamens. Im unteren Teil des Navigationsbereiches befindet sich zusätzlich ein Vorschaubereich des aktuell ausgewählten Bildes.

Symbol-/Werkzeugleiste

Am unteren Rand befindet sich die Symbol- bzw. Werkzeugleiste der sicheren TIFF-Anzeige. Mit den dortigen Symbolen sind weitere Funktionen auswählbar. Die Symbol-/Werkzeugleiste ist nur aktiv, wenn im Navigationsbereich der Eintrag für ein Bild ausgewählt wurde. Bei Auswahl der Bild- und Zusatzinformationen (Anklicken des Dateinamens), ist dieser Bereich inaktiv und ausgegraut. Die Symbole ermöglichen die Ausführung weiterer Funktionen innerhalb der sicheren Anzeige. Ihre Verwendung wird in den kommenden Abschnitten detailliert beschrieben.

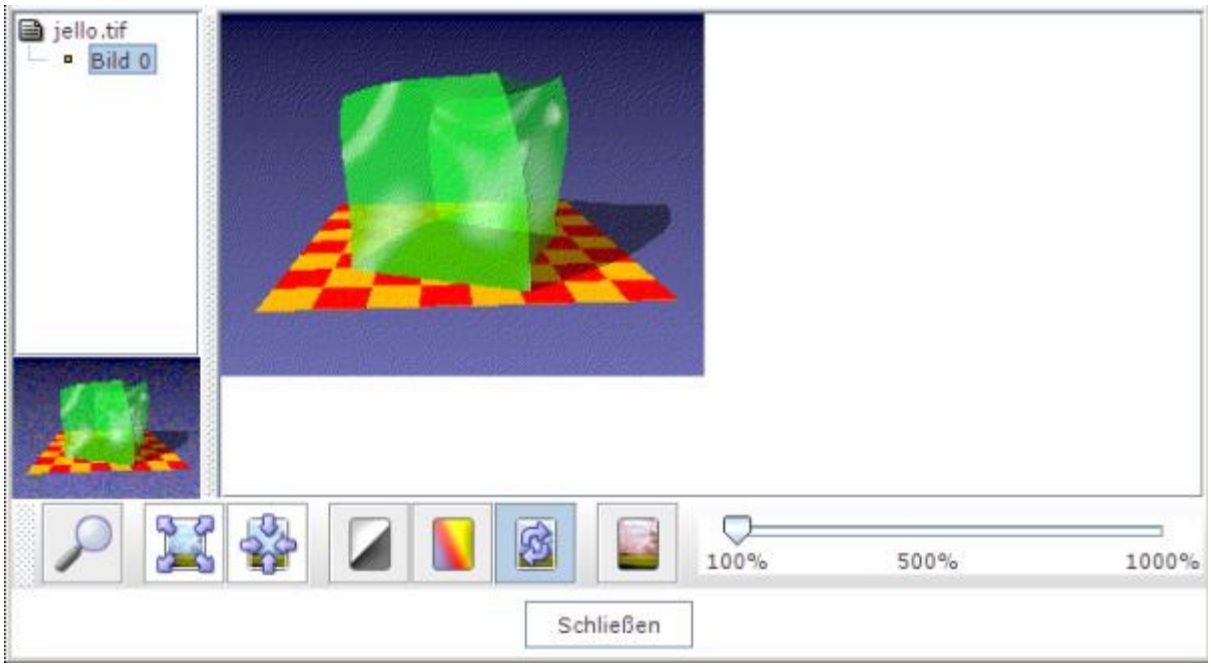


Abbildung 24: Aufbau der sicheren TIFF-Anzeige (Trusted TIFF-Viewer)

7.3.2 Funktionen und Menüführung der sicheren TIFF-Anzeige

Zur sicheren Anzeige von TIFF-Dokumenten gehören sowohl das Bild selbst als auch die nicht sichtbaren, beschreibenden Inhalte des TIFF-Dokuments. Mit Öffnen eines TIFF-Dokuments gelangen Sie zunächst in die sichere Anzeige für das erste gefundene Bild. Dieses wird Ihnen im Anzeigebereich in seiner Normaldarstellung angezeigt.

Auf das gewählte Bild können unter Verwendung der Buttons in der Symbol- und Werkzeugleiste verschiedene Funktionen ausgeführt werden, um die Bilddarstellung zu verändern. Diese Funktionen dienen dazu, eventuell vorhandene und in der Normaldarstellung nicht sichtbare Inhalte aufzudecken.

7.3.2.1 Veränderung der Bilddarstellung

Betrachtet man die Symbole der Werkzeugleiste von links nach rechts, finden sich folgende Funktionen, siehe auch Abbildung 27.

Lupe

Mit der Lupenfunktion können Teile des Bildes vergrößert werden. Klicken Sie dazu auf den Lupe-Button. Innerhalb der Bilddarstellung wird ein eingerahmter, vergrößerter Bereich sichtbar. Sie können diesen Bereich mit gedrückter, linker Maustaste über das Bild bewegen.

	**Hinweis**: Bitte beachten Sie, dass eine Darstellung jedes einzelnen Pixels (Bildpunkt) nur möglich ist, wenn der Vergrößerungswert >300 % ist. Verwenden Sie dazu die Zoomfunktion. Bei Werten <300 % werden Bilder geglättet, d. h. auch mit der Lupenfunktion kann nicht jedes einzelne Pixel dargestellt werden.

Anzeigegröße

Mit diesem Symbol kann die angezeigte Größe des gewählten Bildes auf die aktuelle Fenstergröße angepasst werden. Gegenüber der Normaldarstellung wird das ausgewählte Bild verkleinert oder vergrößert.

Normaldarstellung

Mit diesem Symbol wechseln Sie zur Originalgröße des gewählten Bildes zurück.

Schwellwertverschiebung

Mit Aktivierung der Funktion wird eine Zusatzleiste eingeblendet, die eine Werteskala von -255 bis +255, sowie einen Start-Button enthält, siehe Abbildung 25. Verschieben Sie über die Startfunktion oder direkt mit dem Schieberegler den Schwellwert des gewählten Bildes.

Als Schwellwert wird in der Bildverarbeitung ein Wert bezeichnet, mit dessen Hilfe man farbliche Abgrenzungen in Rasterbildern definiert, z. B. bei der Binarisierung der Grenzwert zwischen Schwarz und Weiß.

Der Schieberegler legt hierbei eine Zahl "t" zwischen -255 und +255. Entsprechend dieser Zahl wird nun die Farbe jedes Pixels wie folgt verändert:

1. Ist t > 0, so werden alle Farbkomponenten, deren Wert größer als t ist, beibehalten. Jeder Wert kleiner oder gleich t wird durch 0 ersetzt.
2. Ist t < 0, so bleiben alle Farbkomponenten, deren Wert kleiner als 255+t ist, unverändert. Jeder Wert größer oder gleich 255+t wird durch 255 ersetzt.

Beispiel: Die Farben mit den RGB-Werten (234, 233, 0) und (233, 234, 0) sind beide gelb und mit bloßem Auge nicht unterscheidbar. Bei der Schwellwerteinstellung t = 233 werden die Farben zu (234, 0, 0) und (0, 234, 0), also rot und grün und sind damit deutlich zu unterscheiden. Bei Einstellung t=0 erscheint das Bild in den Originalfarben, bei t=-255 wird es komplett weiß und bei t=255 komplett schwarz dargestellt.

Die Schwellwertanzeige erfolgt immer mit der gleichen Anzahl von Farbkanälen, die auch das originale Bild hat. Farbige Bilder werden also auch hier farbig dargestellt, da diese Darstellung einen höheren Informationsgehalt als ein Schwarz-Weiß-Bild hat. Die Farben im obigen Beispiel könnten von einer einfachen Schwarz-Weiß-Anzeige mit einstellbarem Schwellwert nicht unterschieden werden. Handelt es sich bei dem betrachteten Bild bereits um ein Schwarz-Weiß- oder Graustufenbild, so bleibt die Anzeige stets schwarz-weiß.

Im Ergebnis können so selbst minimale, mit bloßem Auge nicht sichtbare Kontraste in Bildern durch Schwellwertverschiebung deutlich hervorgehoben werden.

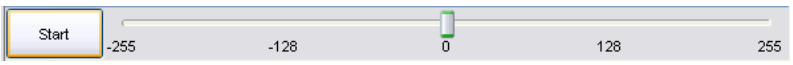


Abbildung 25: Werteskala zur Schwellwertverschiebung

Farbwertverschiebung

Mit Aktivierung des Symbols wird ebenfalls eine zusätzliche Leiste eingeblendet, die neben einem Start-Button je eine Werteskala von -255 bis +255 für die Farben rot, grün und blau enthält, siehe nächste Abbildung. Verwenden Sie die Startfunktion oder die Schieberegler, um die Farbwerte des Bildes zu verändern.

Für jede Farbkomponente jedes Pixels wird, wie im vorangegangenen Abschnitt beschrieben, ein Schwellwert-Filter angewandt. Diesmal können jedoch mit den drei Schiebereglern eigene Schwellwerte für die Primärfarben Rot-, Grün- bzw. Blau-Kanal definiert werden. Dadurch können gezielt einzelne Farbkanäle ausgeblendet werden, sodass z. B. auch Nutzer mit Rot-Grün-Sehschwäche feinste Abstufungen sehen können.

Handelt es sich bei dem betrachteten Bild bereits um ein Schwarz-Weiß- oder Graustufenbild, steht diese Funktion nicht zur Verfügung.

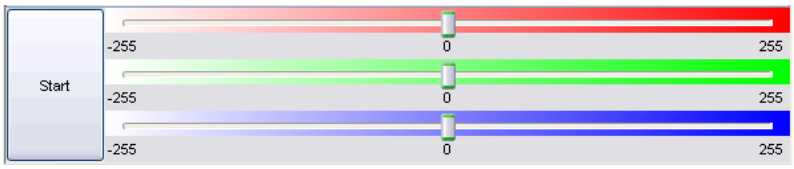


Abbildung 26: Werteskala zur Farbwertverschiebung

Normaldarstellung

Verwenden Sie diese Funktion, um zur Ursprungsansicht des Bildes zurück zu gelangen. Eine Aktivierung beinhaltet die Rückkehr zur 1:1-Darstellung des Bildes sowie die Ausschaltung der Lupenfunktion und Rückstellung bei Falschfarben, Schwell- oder Farbwertverschiebungen.

Falschfarbendarstellung

TIFF-Dokumente können über eigene Farbpaletten oder -tabellen verfügen. Für Bilder mit RGB-Paletten besteht die Möglichkeit, allen Paletteneinträgen einen zufälligen Farbwert zuzuweisen. Hierüber können Informationen sichtbar gemacht werden, die im Originalbild aufgrund zu geringer Helligkeits- oder Farbkontraste nicht sichtbar sind. Die Ersetzung aller Farben ist für den Anwender schneller und einfacher zu handhaben, als die Suche nach geeigneten Schwellwerten.

Für die Erzeugung von Fehlfarben wird die notwendige Anzahl von Farbwerten aus einer festgelegten Folge von Farbwerten ausgewählt. Diese Folge ist durch eine Vorschrift definiert, wie aus einem Farbwert der nachfolgende berechnet wird, und enthält hinreichend viele verschiedene Farben (aktuell 15.357.184).

Ausgewählt werden, von einer zufälligen Farbe beginnend, die nach der Vorschrift folgenden Farbwerte. Die Auswahl erfolgt so, dass bei Paletten bis zu 1024 Einträgen die Farben paarweise möglichst verschieden aussehen. Im Allgemeinen können diese Fehlfarben mit bloßem Auge deutlich unterschieden werden.

Zoomfunktion

Die Verwendung der Zoomfunktion ermöglicht eine Größenveränderung des gesamten Bildes. Ein Zoomen ist bis zu einer Vergrößerung von maximal 1000 % gegenüber der Ursprungsansicht möglich. Verwenden Sie die Zoomfunktion, um Bildglättungen auszuschließen und einzelne Pixel sichtbar zu machen. Die Zoomfunktion steht nur in der Normaldarstellung zur Verfügung.

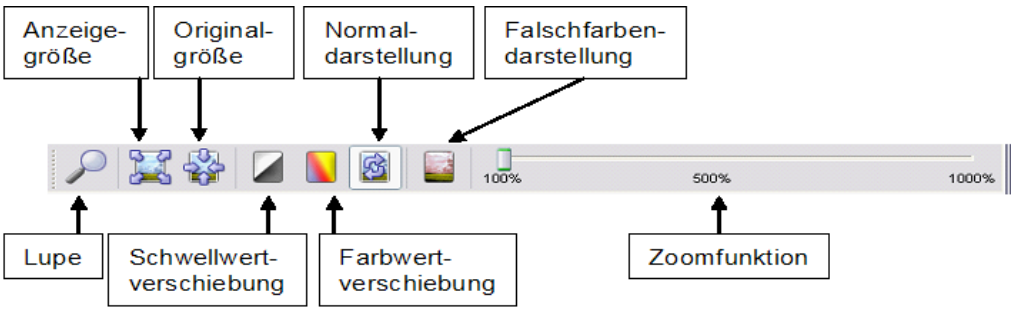


Abbildung 27: Symbolleiste sichere TIFF-Anzeige

	**Hinweis**: Der Schieberegler (bei Zoomfunktion, Schwellwert- oder Farbwertveränderungen) kann mit der Maus oder - sofern sichtbar - automatisch über den Start-Button verschoben werden. Ggf. ist diese Verschiebung jedoch zu grob bzw. zu schnell, um Einzelschritte auszuführen. Klicken Sie daher zunächst auf das Feld mit dem

	jeweiligen Schieberegler, um es zu aktivieren (eine Aktivierung ist durch einen gestrichelten Rahmen erkennbar) und verwenden Sie anschließend die Cursortasten <-- und -->, um Einzelverschiebungen durchzuführen.

7.3.2.2 Bildinformationen, nicht referenzierte Datenbereiche und Bildränder

TIFF-Dokumente beinhalten neben dem Bild selbst weitere, zunächst nicht sichtbare Informationen. Diese können bspw. der Beschreibung dienen oder aber über aktive Inhalte verfügen. Um Manipulationsversuche auszuschließen, werden diese Zusatzinformationen ebenfalls angezeigt.

Klicken Sie in der Navigationsleiste der sicheren Anzeige auf den Dokumentnamen, um eine Übersicht der Bild- und Zusatzinformationen des TIFF-Dokuments zu erhalten. Die Informationen werden innerhalb zweier Registerkarten dargestellt:

- Register "Bildinformationen"
- Register "nicht referenzierte Datenbereiche"

Bildinformationen

Mit dem Reiter "Bildinformationen" werden alle Tags des gewählten TIFF-Dokuments angezeigt. Diese Tags können Meta- oder Zusatzinformationen beinhalten, die ebenfalls im TIFF-Dokument gespeichert sind. In der Mehrzahl dienen sie zur Speicherung von Bildern, können aber auch weitere Texte oder Informationen enthalten.

Die Übersicht im linken Bereich zeigt standardmäßig alle gefundenen Tags in Listenform an. Mit Auswahl eines Tags werden rechts daneben die Detailinformationen angezeigt. Folgende Detailinformationen werden angezeigt:

- **Typ**: Typinformation über den Tag
- **Hex**: Darstellung des Typs als Hexadezimalwert
- **ASCII**: Darstellung des Typs in plain-text
- **Int**: Darstellung des Typs als Ganzzahl (sofern möglich)

Unbekannte Tags und Tags vom Typ ASCII werden als verdächtig eingestuft, da hier weitere Inhalte versteckt sein können. Wählen Sie unter Verwendung der folgenden zwei Radiobuttons im unteren Bereich, ob Sie

- "Alle" oder
- "Nur Verdächtige"

Tags angezeigt bekommen möchten:

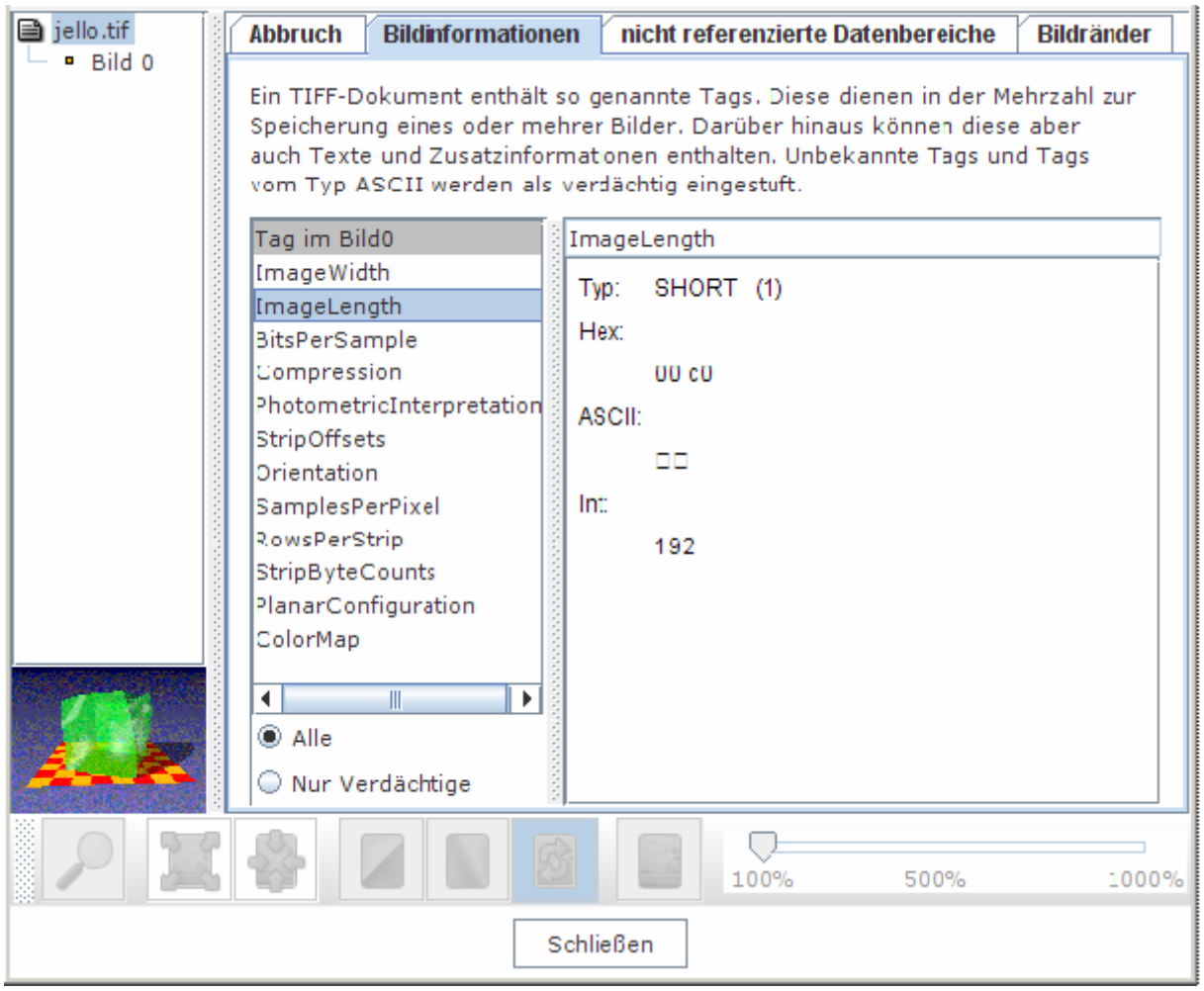


Abbildung 28: Sichere Anzeige der Bildinformationen

Nicht referenzierte Datenbereiche

Neben Tags werden in TIFF-Dokumenten sogenannte Datenbereiche referenziert. Diese Datenbereiche sind ähnlich wie ein Inhaltsverzeichnis zu sehen. Jeder Bereich des TIFF-Dokuments ist über dieses Verzeichnis referenziert. In der Registerkarte "nicht referenzierte Datenbereiche" werden diese Bereiche aufgelistet. Mit Auswahl eines Datenbereichs werden rechts daneben Detailinformationen angezeigt.

Folgende Detailinformationen werden angezeigt:

- **Hex**: Darstellung des Datenbereichs als Hexadezimalwert
- **ASCII**: Darstellung in plain-text

Wählen Sie unter Verwendung der zwei Radiobuttons im unteren Bereich, ob Sie

- "Alle" oder
- "Nur Verdächtige"

Datenbereiche angezeigt bekommen möchten. Technisch bedingte, unreferenzierte Datenbereiche werden als unverdächtig angesehen und in der Auswahl "Nur Verdächtige" nicht mit aufgeführt.

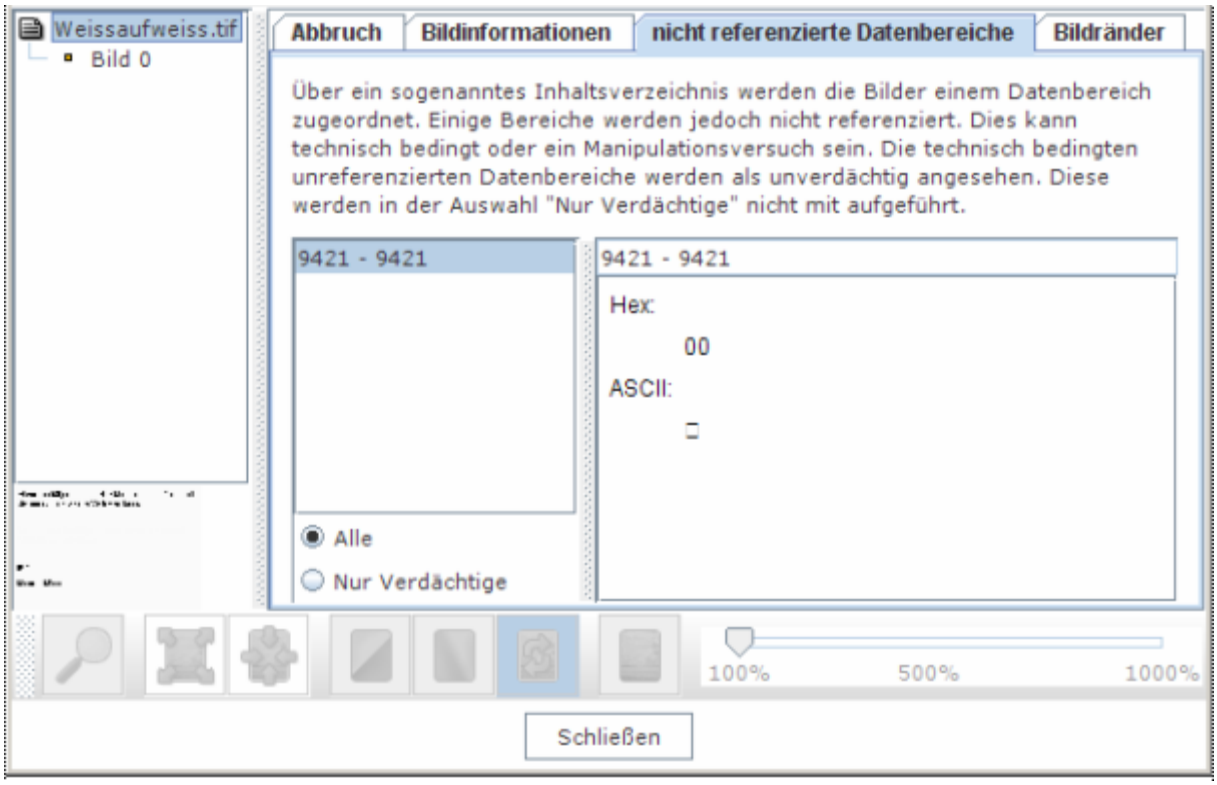


Abbildung 29: Sichere Anzeige der nicht referenzierten Datenbereiche

Bildränder

Wie entstehen Ränder bei TIFF-Dateien? Der Bildbereich einer TIFF-Datei ist entweder in Streifen (Stripes) oder Kacheln (Tiles) aufgebaut. Bei einer TIFF-Datei ist in jedem Streifen oder jeder Kachel Platz für dieselbe Menge an Pixeln. Liegt beispielsweise in einer TIFF-Datei, die in Streifen organisiert ist, eine Streifenhöhe von 50 Pixeln vor und hat das TIFF-Bild eine Höhe von 230 Pixeln, so sind die ersten vier Streifen mit jeweils 50 Pixeln in der Höhe gefüllt und der fünfte Streifen mit 30 Pixeln. Die im fünften Streifen verbleibenden 20 Pixel sind der Rand.

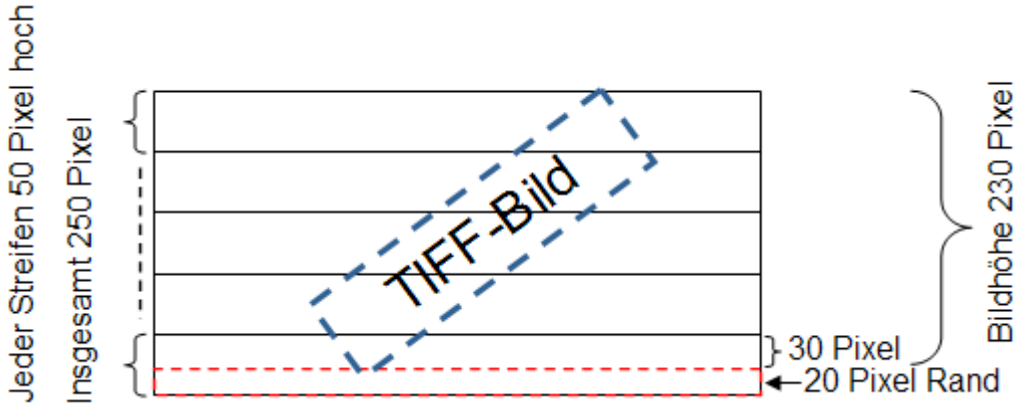


Abbildung 30: Beispiel für den schematischen Aufbau einer TIFF-Datei mit Rand

Bei einer TIFF-Datei, für die ein Rand ausgewiesen wird, muss davon ausgegangen werden, dass dieser potenziell verdächtige Elemente enthält. Dies liegt unter anderem an daran, dass im Datenstrom einer TIFF-Datei die Streifen nicht zwangsläufig in der nummerierten Reihenfolge vorliegen und durch die Möglichkeit der Kompression von TIFF-Dateien ist die Menge der Bytes pro Streifen, respektive Kachel, in der überwiegenden Menge der Fälle

unterschiedlich. Dies macht eine Aussage über den Inhalt eines Bildrands schwierig bis unmöglich.

Nur wenn der Warndialog (siehe Kapitel 7) nicht angezeigt wird und die Ränder im Register "Bilderränder" die Größe "0 px" haben, ist die TIFF-Datei nicht manipuliert. Ist einer der Ränder oder sind beide größer als "0 px", so besteht die Gefahr, dass die TIFF-Datei manipuliert ist. Die folgende Abbildung zeigt die sichere TIFF-Anzeige mit dem Register "Bildränder".

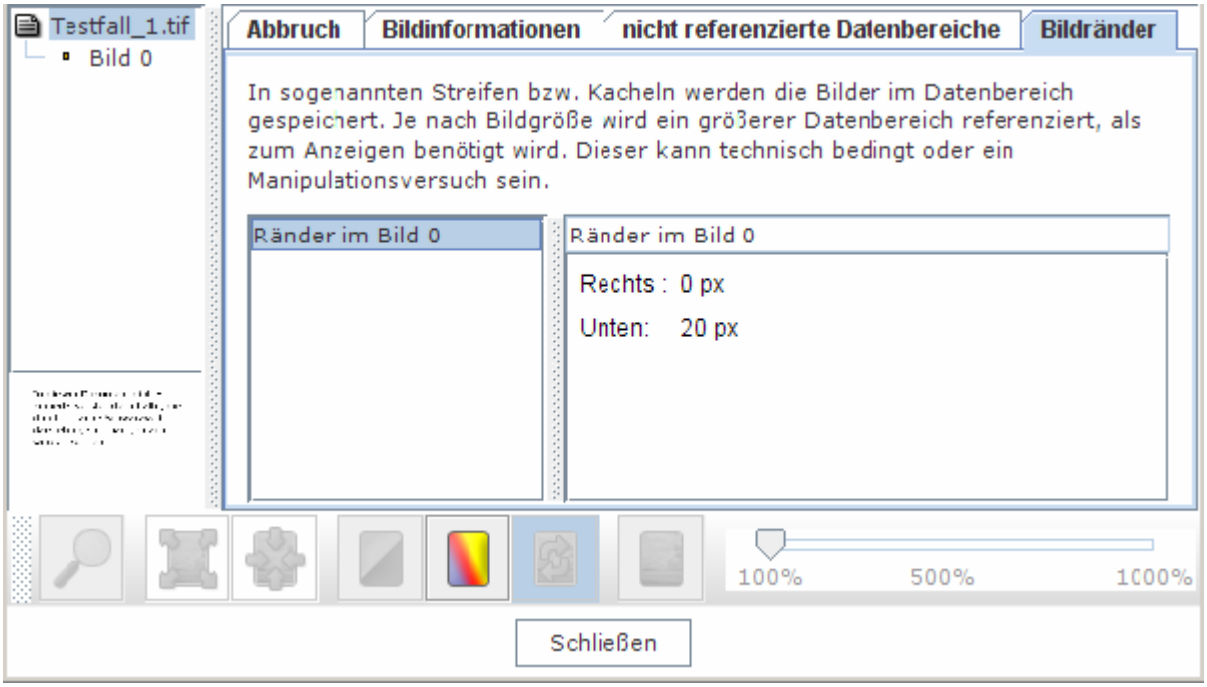


Abbildung 31: Sichere TIFF-Anzeige mit dem Register Bildränder

8 Sichere XML-Anzeige

Die sichere XML-Anzeige wird immer verwendet, wenn Sie XML-Dateien aus der WebEdition heraus öffnen.

Was ist XML?

Die Extensible Markup Language XML ist, ähnlich wie HTML, eine Auszeichnungssprache, bei der Daten durch sogenannte XML-Tags hierarchisch strukturiert und maschinenlesbar abgelegt werden. Da XML-Dateien überwiegend aus Textzeichen bestehen, sind sie prinzipiell auch menschenlesbar. Der Standard XML legt allerdings nur den grundsätzlichen Aufbau solcher Datenstrukturen fest.

Aufgaben der sicheren XML-Anzeige

Mit der sicheren XML-Anzeige können Sie zu signierende sowie signierte XML-Dateien einsehen. Die sichere XML-Anzeige übernimmt dabei folgende Aufgaben:

- **Darstellung der Originaldaten:** Der Inhalt der zu signierenden oder signierten Datei wird über eine bewertete sichere Anzeige dargestellt, optional geschieht dies mit einer verbesserten Lesbarkeit.
- **Darstellung des Inhalts:** Bekannte Fachformate können in eine deutlich besser lesbare Textform überführt werden. Diese vertrauenswürdige Überführung extrahiert den Inhalt und stellt ihn als einfach lesbaren Text dar.
- **Reproduzierbarkeit der vertrauenswürdigen Darstellung:** Es wird sichergestellt, dass die Anzeige von Fachformaten in der aufbereiteten Form bei der Signaturerstellung und bei der Verifikation identisch ist.

Was wird angezeigt?

Mit dem Secure XML Viewer können prinzipiell alle XML-Dateien vor dem Anbringen einer Signatur angezeigt werden. Auch die Anzeige signierter XML-Dateien wird unterstützt, bei denen die Signatur eingebettet ist oder als separate Datei vorliegt. Liegt eine XML-Datei in einem Fachformat vor, das der sicheren XML-Anzeige bekannt ist, wird der Inhalt über eine Transformation aufbereitet und zusätzlich in einer für Menschen besser lesbaren Darstellung angezeigt. Bei einer signierten XML-Datei werden zusätzlich Informationen zur Signatur dargestellt. Wird die sichere XML-Anzeige nach einer Verifikation aufgerufen, wird zusätzlich das zugehörige Prüfprotokoll angezeigt.

Fachformat

Ein Fachformat für XML-Dateien besteht aus einer XML-Schemadatei, einem XML-Stylesheet und einem Regelwerk.

- **XML-Schemadatei**: Damit XML-Dateien maschinenlesbar oder von unterschiedlichen Programmen verarbeitbar sind, gibt die Schemadatei vor, welche XML-Elemente an welchen Stellen vorkommen dürfen und welche Daten sie enthalten können. Mit der XML-Schemadatei kann geprüft werden, ob eine XML-Datei Schema-konform ist oder von den Vorgaben des Schemas abweicht.

- **XML-Stylesheet**: Um eine XML-Datei in eine besser lesbare Form umwandeln zu können, wird ein XML-Stylesheet benötigt, dass die Gestaltung des Dokumenteninhalts vorgibt. Mit dem Stylesheet und der XML-Datei kann ein entsprechendes Transformationsprogramm den Dokumenteninhalt in der sicheren XML-Anzeige erstellen.
- **Regelwerk**: Das Regelwerk gibt innerhalb eines Fachformats vor, welche Tests vor einer sicheren Anzeige durchgeführt werden sollen. Das Ergebnis entscheidet darüber, ob eine sichere Anzeige des Dokumentinhalts erstellt wird. Die Kriterien sind beispielhaft in nächsten Kapitel im Abschnitt "Registerkarte Meldungen" erklärt.

Nur wenn ein Fachformat der sicheren XML-Anzeige bekannt ist, kann eine sichere und vertrauenswürdige aufbereitete Darstellung einer zu signierenden XML-Datei angeboten werden und die Reproduzierbarkeit der Darstellung bei der Signaturprüfung sichergestellt werden.

Bewertete sichere Anzeige

Bei allen XML-Dateien wird zunächst nach einem internen Regelwerk eine Bewertung durchgeführt, ob eine sichere und vertrauenswürdige Darstellung möglich ist. Es wird überprüft, ob nichtdarstellbare Zeichen enthalten sind und ob die Struktur die Regeln von XML korrekt einhält. Bei Nichteinhaltung dieser Regeln erfolgt keine Anzeige der Daten.

Bei zu signierenden bekannten Fachformaten, siehe Abschnitt Fachformat, findet zusätzlich eine Bewertung anhand der XML-Schemadatei und dem Regelwerk des Fachformats statt, um eine sichere Anzeige zu gewährleisten. Nur wenn nicht gegen wichtige Kriterien verstoßen wird, ist eine vertrauenswürdige Überführung in ein besser lesbares Format möglich. Es wird beispielsweise geprüft, ob alle Daten sichtbar sind. Befindet sich etwa weiße Schrift auf weißem Hintergrund oder sind aktiven Links enthalten oder wird die Anzeige von Daten explizit unterdrückt, erfolgt keine Transformation. In diesem Fall kann nur die XML-Datei selbst angezeigt werden.

Reproduzierbarkeit der Darstellung

Die Reproduzierbarkeit der Darstellung wird wie folgt gewährleistet. Die Signatur der XML-Datei umfasst zusätzlich das verwendete XML-Stylesheet sowie einen Hashwert, der über die transformierten Daten erzeugt wird. Wenn diese signierte Datei mit der sicheren XML-Anzeige geöffnet wird, werden die Inhalte unter Verwendung des beigelegten XML-Stylesheets wieder in die besser lesbare Form transformiert, vorausgesetzt, die fachformatunabhängige Bewertung erfolgreich durchgeführt wurde. Anschließend wird über die transformierten Daten wieder ein Hashwert gebildet, der mit dem Hashwert aus der signierten Datei verglichen wird. Stimmen beide Hashwerte überein, ist sichergestellt, dass die Anzeige der signierten Inhalte identisch mit der Anzeige vor der Signaturerstellung ist. Stimmen die Hashwerte nicht überein, werden die aufbereiteten Inhalte nicht angezeigt. Es ist dann nur die Anzeige der XML-Datei möglich.

Hinweis: Eine Abweichung des Hashwerts nach der Transformation der XML-Datei in die besser lesbare Darstellung ist möglich. Die Transformation ist unter anderem auch abhängig vom Betriebssystem des Anwenders. Da bei einer Abweichung nicht sichergestellt werden kann, dass für die Person, die die Signatur erstellt hat, den Inhalt genauso angezeigt wurde, wie für die Person die die signierte Datei empfangen hat, wird in diesem Fall nur die XML-Datei angezeigt. Eine Abweichung des Hashwerts für die transformierte Darstellung bedeutet nicht, dass die XML-Datei selbst geändert ist. Dies würde bereits bei der Signaturprüfung angezeigt werden.

Erhöhung der Lesbarkeit

Bei der Anzeige der Originaldaten werden direkt die XML-Strukturen dargestellt. Hier besteht die Möglichkeit, die Lesbarkeit dieser XML-Strukturen durch Texthervorhebungen und Formatierungen zu erhöhen. Diese Möglichkeiten werden als Checkboxen angeboten.

- **Texthervorhebungen**: Als Vorgabe ist diese Checkbox ist ausgewählt. Damit werden die Daten farblich hervorgehoben, um Inhalte und Strukturbeschreibung besser unterscheiden zu können. Bei sehr großen XML-Dateien ist dies nicht möglich.
- **Formatierung**: Als Vorgabe ist diese Checkbox ist ausgewählt. Es werden die angezeigten Daten in eine Struktur überführt, die die Lesbarkeit erhöht. Dazu werden an den Grenzen der XML-Tags Zeilenumbrüche eingefügt und es wird die Hierarchie der XML-Tags durch einrücken kenntlich gemacht. Bei sehr großen XML-Dateien ist dies nicht möglich.
- Des Weiteren werden leere XML-Tags immer in der Kurzform dargestellt - aus `<tag></tag>` wird `<tag/>`.

8.1 Aufruf der sicheren XML-Anzeige

Die sichere XML-Anzeige wird über die Dateiauswahl aufgerufen. Die Dateiauswahl listet alle Dateien auf, die Sie zum Signieren oder Verifizieren in den Governikus Signer geladen haben. Am Ende jeder Zeile befindet sich das Lupen-Symbol. Befindet sich in der Zeile eine XML-Datei, wird beim Anklicken des Lupen-Symbols die sichere XML-Anzeige mit dieser XML-Datei aufgerufen.

8.2 Registerkarten der sicheren XML-Anzeige

Die sichere XML-Anzeige verfügt über mehrere Registerkarten. Die Anzahl und Auswahl der verfügbaren Registerkarten ist abhängig von der XML-Datei und dem Kontext in dem die sichere XML-Anzeige aufgerufen wird. Die folgenden Registerkarten können angezeigt werden.

Registerkarte Dokumenteninhalt

Die Registerkarte "Dokumenteninhalt" enthält die aufbereitete Darstellungsform des Inhalts und kann nur angezeigt werden, wenn der sicheren XML-Anzeige das Fachformat der XML-Datei bekannt ist und bei der Auswertung der Sicherheitskriterien keine Fehler gefunden wurden. Auch wenn der Dokumentinhalt zu lang ist, kann die Ansicht "Dokumentinhalt" nicht erstellt werden. Das Fachformat gibt unter anderem auch vor, wie die XML-Datei signiert wird. Es kann die gesamte XML-Datei oder nur ein Teil davon signiert werden. Die Registerkarte "Dokumenteninhalt" zeigt den Bereich der Daten an, der signiert werden kann bzw. signiert wurde.

Registerkarte XML

Diese Registerkarte wird nur angezeigt, wenn eine unsignierte XML-Datei dargestellt wird und zeigt die originalen zu signierenden XML-Daten. Wenn kein Fachformat bekannt ist, wird immer die gesamte XML-Datei angezeigt. Ist das Fachformat bekannt, gibt das Fachformat vor, wie die XML-Datei signiert wird. Es kann vom Fachformat auch vorgegeben werden, dass nur ein Teil der XML-Datei signiert wird. In diesem Fall wird nur der zu signierende Teil angezeigt. Diese Registerkarte verfügt über die Checkboxen Texthervorhebungen und Formatierung, siehe Einleitung zur sicheren XML-Anzeige.

Registerkarte Meldungen

Auf dieser Registerkarte werden alle Meldungen angezeigt, die beim Aufruf der sicheren XML-Anzeige und bei der Auswertung der Sicherheitskriterien entstanden sind.

- : Der grüne Kreis mit weißem Haken steht für erfolgreiche Prüfungen. Sie können hier nachlesen, welche Prüfungen erfolgreich durchgeführt wurden.
- : Der gelbe Kreis mit grauem Ausrufezeichen steht für Warnungen. Sie können hier nachlesen, welche Prüfungen zu Problemen geführt haben. Wenn kein Fachformat für die XML-Datei zur Verfügung steht, kann die Datei nicht sicher angezeigt werden, dann stehen nur die Registerkarten "Meldungen" und "XML" in der sicheren XML-Anzeige zur Verfügung.
- : Der rote Kreis mit schwarzem Kreuz steht für Fehler. Hier werden die Fehlergründe gelistet. Es können Fehler festgestellt werden, die dazu führen, dass in der sicheren XML-Anzeige nur die Registerkarte "Meldungen" angezeigt wird. In diesem Fall kann das Dokument nicht sicher angezeigt werden. Wenn Sie die sichere XML-Anzeige schließen, können Sie die XML-Datei danach mit dem Standardprogramm anzeigen lassen, das auf Ihrem Rechner mit der Dateiendung XML verbunden ist.

Registerkarte verwendetes Stylesheet

Diese Registerkarte enthält das zur Aufbereitung der Daten verwendete XML-Stylesheet in Form einer XML-Datenstruktur. Sie wird nur dann angezeigt, wenn zur XML-Datei ein Fachformat existiert, das der sicheren XML-Anzeige bekannt ist. Dieser Inhalt wird im Falle einer Signatur mitsigniert, um eine immer gleiche Darstellung sicherzustellen. Diese Registerkarte verfügt über die Checkboxen Texthervorhebungen und Formatierung, siehe Einleitung zur sicheren XML-Anzeige.

Registerkarte signierter Teil des XML

Diese Registerkarte wird angezeigt, wenn die XML-Datei bereits signiert wurde. Sie zeigt den signierten Teil der XML-Datei als XML-Struktur. Der signierte Teil kann ein Teil oder die ganze Datei sein. Diese Registerkarte verfügt über die Checkboxen Texthervorhebungen und Formatierung, siehe Einleitung zur sicheren XML-Anzeige.

Registerkarte Signatur

Diese Registerkarte wird nur angezeigt, wenn die dargestellte XML-Datei bereits signiert ist und zeigt im oberen Bereich Eigenschaften der Signatur an, wie den Signaturzeitpunkt, den Signaturalgorithmus und den Hash-Algorithmus. Zudem wird ausgewiesen, ob die Signatur zu den signierten Daten passt. Darunter folgen die Informationen zum Signaturzertifikat. Der Abschnitt "Details" kann aufgeklappt werden und zeigt dann weitere Informationen zum Zertifikat.

Registerkarte Gesamtdokument

Diese Registerkarte wird nur angezeigt, wenn die XML-Datei signiert ist. In dieser Registerkarte wird das gesamte Dokument angezeigt, da in der Registerkarte "Signierter Teil des XML", siehe oben. möglicherweise nur ein Teil des Dokuments angezeigt wird. Diese Registerkarte verfügt über die Checkboxen Texthervorhebungen und Formatierung, siehe Einleitung zur sicheren XML-Anzeige.

Registerkarte Prüfprotokoll

Diese Registerkarte wird nur angezeigt, wenn die XML-Datei signiert ist und im Governikus Signer eine Verifikation durchgeführt wurde. In dieser Registerkarte wird das Ergebnis der

Signaturprüfung dargestellt, also welchen Status das Signaturzertifikat zum Zeitpunkt der Signaturanbringung hatte.

9 Verschlüsseln mit der WebEdition

Mit dieser Funktion können Sie Dateien verschlüsseln. Eine Erklärung zum Verschlüsseln finden Sie im Kapitel 12.5. Im Folgenden werden die Dialoge erklärt, die für die Funktion "Verschlüsseln" existieren. Bitte beachten Sie, dass Dialogseiten ganz oder teilweise ausgegraut sein können oder gar nicht angezeigt werden, wenn die dort vorhandenen Einstellungen bereits von Ihrem Diensteanbieter festgelegt wurden.

9.1 Dateiauswahl

Der Dialog Dateiauswahl kann ausgeblendet sein. In diesem Fall wird die WebEdition bereits mit ausgewählten Dateien gestartet. Auf der rechten Seite finden Sie eine Liste, die anfangs leer sein kann. Sie können beliebig viele Dateien aus verschiedenen Verzeichnissen auswählen. Die folgenden Möglichkeiten stehen Ihnen zur Verfügung, um Dateien hinzufügen.

Drag-and-drop

Markieren Sie eine oder mehrere Dateien im Dateimanager und ziehen Sie die Auswahl bei gedrückter linker Maustaste in die Liste der WebEdition.

Button "Datei hinzufügen"

Mit dem Button "Datei hinzufügen" rufen Sie ein Dialogfenster zur Dateiauswahl auf. Navigieren Sie in das gewünschte Verzeichnis, wählen Sie die gewünschten Dateien aus, und klicken Sie auf "Übernehmen". Die Dateiliste enthält nun Ihre Auswahl.

Dateien entfernen

Sie können Dateien auch wieder aus der Dateiauswahl entfernen. Markieren Sie die Dateien, die Sie aus der Dateiauswahl entfernen wollen und klicken Sie dann auf den Button "Ausgewählte Dateien entfernen".

Die Dateiliste

Die Dateiliste listet zeilenweise alle Dateien auf, die zum Verschlüsseln ausgewählt haben.

- Dateiname: In jeder Zeile steht zuerst der Dateiname.
-  : Das Augensymbol wird angezeigt, wenn die Datei vor dem Verschlüsseln angezeigt wurde. Das Symbol ist grau, wenn die Datei noch nicht angezeigt wurde.
-  : Klicken Sie auf das Lupensymbol, um die Datei anzeigen zu lassen. Die Datei wir mit dem Programm angezeigt, dass auf Ihrem Computer mit der Dateiendung verbunden ist.

9.2 Schlüssel wählen

Wählen Sie auf dieser Dialogseite einen Schlüssel. Zur Auswahl steht die Verschlüsselung mit einem Passwort oder mit dem öffentlichen Schlüssel, der entweder aus einem Keystore oder einem Verschlüsselungszertifikat bezogen wird. Eine Erklärung zum Verschlüsseln finden Sie im Kapitel 12.5.

Verschlüsselung mit Passwort

Wenn Sie die Verschlüsselung mit einem Passwort auswählen, werden Sie auf der letzten Dialogseite "Verschlüsseln" zur Eingabe eines Passworts aufgefordert. Diese Verschlüsselung wird immer mit dem Algorithmus "AES 256" durchgeführt.

	**Hinweis**: Bitte beachten Sie, dass Sie das Passwort, das Sie zum Verschlüsseln angeben, auch zum Entschlüsseln benötigen.

Verschlüsselung mit öffentlichem Schlüssel

Alle von Ihnen geladenen öffentlichen Schlüssel werden in einer Liste angezeigt. Diese öffentlichen Schlüssel sind üblicherweise die Ihrer Geschäftspartner, mit denen Sie verschlüsselte Dateien austauschen wollen. Nur Ihre Geschäftspartner sind dann wiederum in der Lage, mit ihren privaten Schlüsseln die Dateien zu entschlüsseln. Sie können auch Ihren eigenen öffentlichen Schlüssel hier hinzufügen, sodass Sie selbst in der Lage sind, die verschlüsselte Datei wieder zu entschlüsseln.

Speicherort des Zertifikats

-  **Zertifikat aus Datei laden**: Wenn Sie einen öffentlichen Schlüssel aus einer Datei laden wollen, klicken Sie auf dieses Symbol und navigieren Sie an die Stelle im Dateisystem, an der dieser Schlüssel abgelegt ist. Keystores haben das Suffix `.p12` oder `.pfx`, Zertifikate haben den Suffix `.cer` oder `.crt`. Ein Keystore enthält ein Zertifikat und das benötigte Schlüsselpaar für die asymmetrische Verschlüsselung. Lesen Sie dazu auch das Kapitel **12.5** über asymmetrische Verschlüsselung.

	**Hinweis**: Nach dem Laden eines Zertifikats aus einem Keystore müssen Sie die PIN für den Zugriff auf diesen Keystore eingeben. Das Laden eines Zertifikats von einer Signaturkarte hingegen erfordert keine PIN-Eingabe.

-  **Signaturkarte**: Diese Auswahl wird nur angezeigt, wenn Sie einen Kartenleser angeschlossen und eine Signaturkarte eingelegt haben. Unter diesem Symbol steht der Name des Kartenlesers, der von der WebEdition erkannt wurde. Sie können bis zu 10 Kartenleser anschließen. Sollten Sie weitere Kartenleser anschließen wollen, lesen Sie zuvor die mitgelieferten Dokumente zu den Systemvoraussetzungen. **Hinweis**: Auf einer Signaturkarte befinden sich Verschlüsselungszertifikate. Es wird nur der öffentlichen Schlüssel des Verschlüsselungszertifikats angezeigt.

	**Hinweis**: Sind im Dialogabschnitt "Speicherort des Zertifikates" Symbole von Kartenlesern **ausgegraut**, sind diese **nicht** auswählbar. Wenn Sie eine Signaturkarte benutzen wollen, müssen Sie diese in einen angeschlossenen Kartenleser einlegen. Wenn die Signaturkarte vom Kartenleser eingelesen wurde, ist das Symbol nicht mehr ausgegraut und auswählbar.

Hinweis: Öffentlicher Schlüssel einer Signaturkarte (Verschlüsselungszertifikat)

Dateien werden mit einem öffentlichen Schlüssel verschlüsselt und können danach nur noch mit dem privaten Schlüssel entschlüsselt werden. Sie können über das Lupensymbol am rechten Rand der Schlüsselliste den öffentlichen Schlüssel Ihrer Signaturkarte anzeigen und in diesem Anzeigedialog das Verschlüsselungszertifikat abspeichern. Diesen öffentlichen Schlüssel können Sie dann an die Geschäftspartner schicken, mit denen Sie verschlüsselte Dateien austauschen wollen. Sie sind der Einzige, der mit dem zum öffentlichen Schlüssel passenden privaten Schlüssel verschlüsselte Dateien wieder entschlüsseln kann.

Zertifikate wählen

Auf der rechten Seite dieses Dialogabschnitts werden alle öffentlichen Schlüssel der von Ihnen ausgewählten Zertifikate aufgelistet. Markieren Sie hier alle öffentlichen Schlüssel, die Sie zur Verschlüsselung der Dateien benutzen wollen. Fügen Sie hier alle öffentlichen Schlüssel der Geschäftspartner hinzu, für die die verschlüsselten Dateien bestimmt sind.

Hinweis: Wenn Sie eine oder mehrere Dateien für mehrere Geschäftspartner verschlüsseln wollen, markieren Sie hier deren öffentlichen Schlüssel. Die Dateien werden mit allen Schlüsseln so verschlüsselt, dass jeder dieser Geschäftspartner die Dateien mit seinem privaten Schlüssel entschlüsseln kann. Lesen Sie Kapitel **12.5** für weitere Informationen zum Verschlüsseln.

9.3 Zielverzeichnis wählen

Bitte beachten Sie, dass Dialogseiten ganz oder teilweise ausgegraut sein können oder gar nicht angezeigt werden, wenn die dort vorhandenen Einstellungen bereits von Ihrem Diensteanbieter festgelegt wurden.

Dateien zu einem ZIP-Archiv zusammenfügen

Wenn Sie diese Einstellung auswählen, werden beim Verschlüsseln zuerst alle von Ihnen ausgewählten Dateien in einem ZIP-Archiv zusammengefasst. Dieser Packvorgang wird auf der nächsten Dialogseite "Verschlüsseln" durch den Verschlüsseln-Button ausgelöst. Danach wird das ZIP-Archiv verschlüsselt. Es entsteht dabei eine ZIP-Archivdatei mit dem Suffix `.zip.p7m`.

Zielverzeichnis wählen

Im Zielverzeichnis werden die Dateien abgelegt, nachdem Sie die Funktion "Verschlüsseln" ausgeführt haben. Der Dialog bietet Ihnen zwei Optionen. Sie können entweder das Quellverzeichnis nutzen oder ein neues Zielverzeichnis auswählen. Die getroffene Auswahl wird blau umrandet.

- **Quellverzeichnis nutzen**: Diese Einstellung ist die Standardauswahl. Nachdem Sie die Funktionen "Verschlüsseln" angewendet haben, werden die Ergebnisdateien in dasselbe Verzeichnis geschrieben, aus dem die jeweilige Originaldatei stammt.
- **Zielverzeichnis wählen**: Bei dieser Auswahl öffnet sich gleichzeitig ein Auswahldialog, über den Sie ein Verzeichnis festlegen können, in das alle verschlüsselte Dateien abgelegt werden. Der Pfad zum Zielverzeichnis wird danach unter dem Button "Zielverzeichnis wählen" angezeigt.

Lokale Kopie erstellen

Wenn Sie Kopien der verschlüsselten Dateien an einem zusätzlichen Ort speichern möchten, können Sie diesen hier auswählen.

- **Zielverzeichnis wählen**: Wählen Sie über den Button ein Verzeichnis aus, in dem Sie Kopien der verschlüsselten Dateien speichern wollen.
- **Zielverzeichnis löschen**: Wählen Sie den Button mit dem Papierkorbsymbol um das ausgewählte Verzeichnis wieder zu löschen. Wenn Sie das Zielverzeichnis gelöscht haben, werden keine lokalen Kopien in das Zielverzeichnis kopiert.

	**Hinweis**: Bitte beachten Sie, dass die hier getroffenen Einstellungen beim nächsten Programmaufruf der WebEdition nicht mehr vorhanden sind.

9.4 Verschlüsseln

Auf dieser Dialogseite der Funktion "Verschlüsseln" werden die Dateien, die Sie zum Verschlüsseln ausgewählt haben, aufgelistet. Das Verschlüsseln starten Sie mit dem Verschlüsseln-Button unten auf der Seite.

Zufallszahlenerzeugung

Die Verschlüsslungsfunktion benötigt zu Beginn eine Zufallszahl, die normalerweise ohne Ihr Eingreifen im Hintergrund erzeugt wird. In einigen Fällen kann es vorkommen, dass auf Ihrem System keine "ausreichend zufällige" Zufallszahl erstellt werden kann. Um die Qualität der Verschlüsselung nicht zu gefährden, werden Sie diesen Fall durch folgenden Dialog um Mithilfe gebeten:

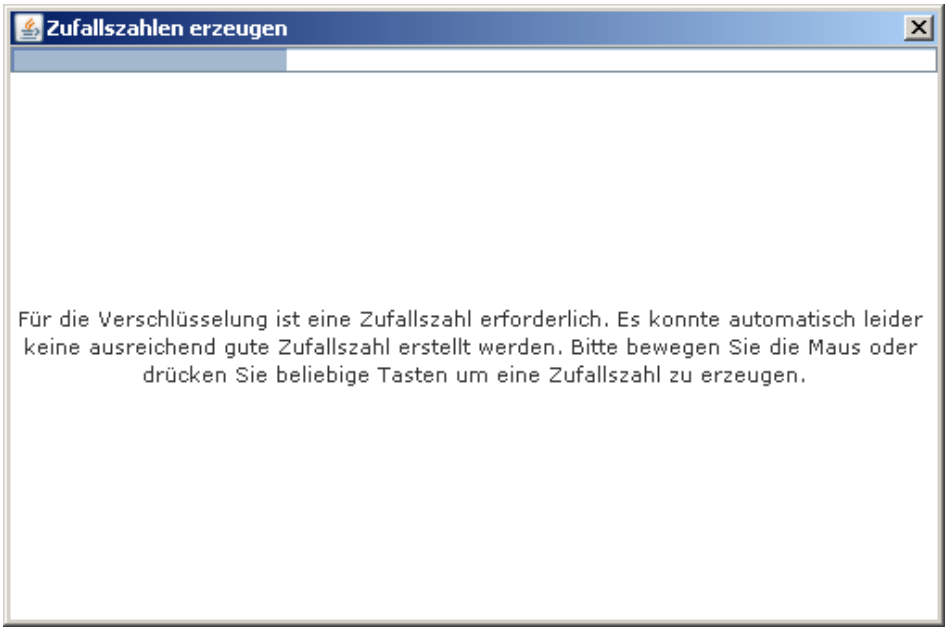


Abbildung 32: Dialog zur Erzeugung einer Zufallszahl für die Verschlüsselung

Durch bewegen des Mauspfeils innerhalb des Dialogfensters oder durch beliebige Tastatureingaben müssen Sie nun "zufällige" Eingaben erzeugen bis der Fortschrittsbalken gefüllt ist und eine Zufallszahl generiert werden konnte. Nach erfolgreicher Erstellung der Zufallszahl schließt sich das Dialogfenster automatisch und die Verschlüsselung wird durchgeführt.

Die Listendarstellung

Die Zeilen in der Listendarstellung haben die folgenden Spalten:

- **Datei**: Zeigt den Namen der Datei an, die verschlüsselt werden soll. Wenn Sie den Mauszeiger über den Dateinamen legen, wird der vollständige Pfad angezeigt.
-  : Das Augensymbol wird angezeigt, wenn die Datei vor dem Verschlüsseln angezeigt wurde. Das Symbol ist grau, wenn die Datei noch nicht angezeigt wurde.
-  : Klicken Sie auf das Lupensymbol, um die Datei anzeigen zu lassen. Die Datei wir mit dem Programm angezeigt, dass auf Ihrem Computer mit der Dateiendung verbunden ist.
- **Status**: Diese Spalte zeigt den Verarbeitungsstatus der Datei an. Diese Meldungen werden angegeben:
  - **Neu**: die Datei wurde noch nicht verarbeitet;
  - **In Arbeit**: die Verarbeitung wird gerade durchgeführt:
  - **Gepackt**: Wenn Sie auf der Dialogseite "Schlüssel wählen" die Option zum Zusammenfassen der Dateien in einer Archiv-Datei ausgewählt haben, wird der Status "Gepackt" angezeigt, wenn die zu verschlüsselnde Datei zur Archiv-Datei hinzugefügt wurde.
  - **Fertig**: die Verarbeitung ist abgeschlossen;
  - **Fehler**: bei der Verarbeitung ist ein Fehler aufgetreten.
- **Ergebnisdatei**: Das Ergebnis des Verschlüsselns ist eine Datei mit der Endung `.p7m`. Bei einer erfolgreichen Verarbeitung sind in dieser Spalte Pfad und Dateiname zu sehen. Wenn Sie auf der Dialogseite "Schlüssel wählen" die Option zum Zusammenfassen der Dateien in einer Archiv-Datei ausgewählt haben, ist die Anzeige in der Spalte Ergebnisdatei wie folgt: Alle Dateien, die den Status "Gepackt" haben, haben keine Ergebnisdatei. Am Ende der Liste wird eine ZIP-Archivdatei mit der Endung `.zip.p7m` samt Pfad angezeigt, die in der Spalte "Datei" keine korrespondierende Datei hat.

Ergebnisdatei vorhanden

Wenn beim Erstellen der Ergebnisdatei bemerkt wird, dass eine Datei mit gleichem Namen im Zielverzeichnis und/oder im Verzeichnis für lokale Kopien bereits vorhanden ist, wird der Dialog "Zieldatei vorhanden" angezeigt. Sie haben hier die Möglichkeit, eine Auswahl zu treffen.

- **Überschreiben**: Die neue verschlüsselte Datei ersetzt die bereits vorhandene.
- **Umbenennen**: Beim Umbenennen wird der Datei das aktuelle Datum im Dateinamen vorangestellt.
- **Abbrechen**: Sie können die Verarbeitung auch abbrechen.

Sollten Sie mehrere Dateien verschlüsseln, besteht beim Überschreiben oder Umbenennen zusätzlich die Möglichkeit, diese Aktion auf alle nachfolgend zu verschlüsselnden Dateien anzuwenden, deren Ergebnisdateien ebenfalls bereits vorhanden sind. Wählen Sie dazu die Option "Aktion für nachfolgende Dateien automatisch durchführen" im selben Dialog.

Diese Option hat keine Auswirkung, wenn Sie "Abbrechen" wählen. In diesem Fall wird der Dialog bei jeder weiteren, bereits vorhandenen Ergebnisdatei erneut angezeigt. Wird die Verarbeitung abgebrochen, wird dies als Fehler gewertet.

Passwort-basierte Verschlüsselung

Wenn Sie auf der Dialogseite "Schlüssel wählen" die Passwort-basierte Verschlüsselung gewählt haben, werden Sie nach dem Auslösen des Verschlüsselungsprozesses durch ein Dialogfenster zur Eingabe eines Passworts aufgefordert. Neben dem Eingabefeld für das Passwort befindet sich ein Feld mit fünf Punkten. Solange Ihr Passwort trivial ist, beispielsweise nur Zahlen und zu wenig Zeichen, werden nur wenige Punkte rot gefüllt. Mit zunehmender Komplexität des Passworts werden die Punkte grün. Wenn alle Punkte grün sind, ist Ihr Passwort ausreichend sicher.

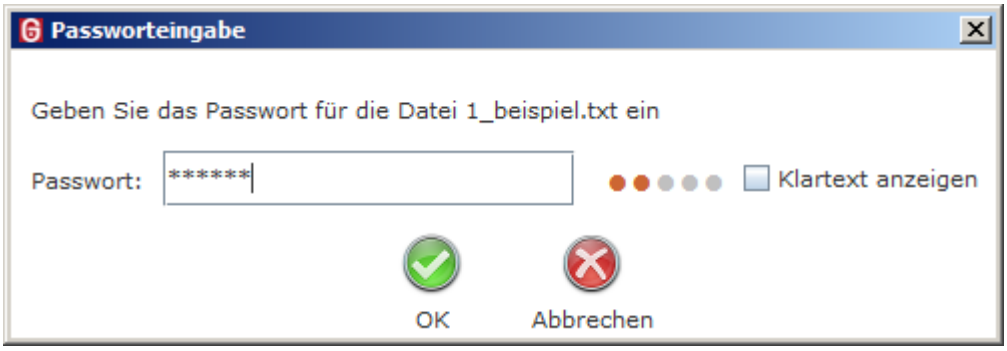


Abbildung 33: Eingabe eines trivialen Passworts - wenige rote Punkte

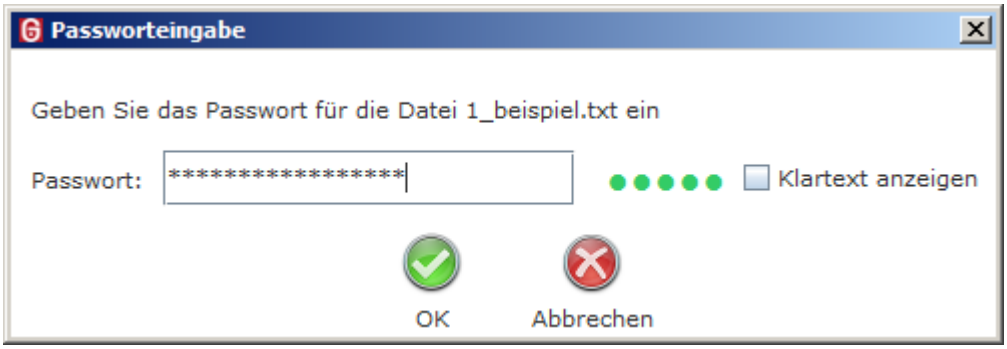


Abbildung 34: Eingabe eines ausreichend sicheren Passworts - alle Punkte grün

Ende des Verschlüsselungsprozesses

Wenn der Verschlüsselungsprozess ohne Fehler durchgeführt werden konnte, beendet sich die WebEdition automatisch. Traten ein oder mehrere Fehler auf, wird dies durch ein Dialogfenster angezeigt. Die WebEdition wird dann mit bestätigen dieses Dialoges beendet. Ihr Dienstanbieter kann festlegen, wie danach verfahren wird. Entweder kehren Sie zur aufrufenden Fachanwendung zurück oder Sie werde auf eine Seite weitergeleitet, die der Dienstanbieter festgelegt hat. Der Dienstanbieter kann auf so einer Seite beispielsweise die Statusmeldungen der WebEdition auflisten. So dass Sie Erfolgs- oder Fehlermeldungen erneut nachlesen können.

10 Entschlüsseln mit der WebEdition

Mit dieser Funktion können Sie Dateien entschlüsseln. Eine Erklärung zum Entschlüsseln finden Sie im Kapitel 12.5. Im Folgenden werden die Dialoge erklärt, die für die Funktion "Entschlüsseln" existieren. Bitte beachten Sie, dass Dialogseiten ganz oder teilweise ausgegraut sein können oder gar nicht angezeigt werden, wenn die dort vorhandenen Einstellungen bereits von Ihrem Diensteanbieter festgelegt wurden.

10.1 Dateiauswahl

Der Dialog Dateiauswahl kann ausgeblendet sein. In diesem Fall wird die WebEdition bereits mit ausgewählten Dateien gestartet. Auf der rechten Seite finden Sie eine Liste, die anfangs leer sein kann. Sie können beliebig viele Dateien aus verschiedenen Verzeichnissen auswählen. Die folgenden Möglichkeiten stehen Ihnen zur Verfügung, um Dateien hinzufügen.

Drag-and-drop

Markieren Sie eine oder mehrere Dateien im Dateimanager und ziehen Sie die Auswahl bei gedrückter linker Maustaste in die Liste der WebEdition.

Button "Datei hinzufügen"

Mit dem Button "Datei hinzufügen" rufen Sie ein Dialogfenster zur Dateiauswahl auf. Navigieren Sie in das gewünschte Verzeichnis, wählen Sie die gewünschten Dateien aus, und klicken Sie auf "Übernehmen". Die Dateiliste enthält nun Ihre Auswahl.

Dateien entfernen

Sie können Dateien auch wieder aus der Dateiauswahl entfernen. Markieren Sie die Dateien, die Sie aus der Dateiauswahl entfernen wollen und klicken Sie dann auf den Button "Ausgewählte Dateien entfernen".

Die Dateiliste

Die Dateiliste listet zeilenweise alle Dateien auf, die zum Verschlüsseln ausgewählt haben. In jeder Zeile steht der Dateiname.

10.2 Schlüssel wählen

Wählen Sie auf dieser Dialogseite einen Schlüssel. Zur Auswahl steht die Entschlüsselung mit einem Passwort oder mit dem privaten Schlüssel, der entweder aus einer Keystore-Datei oder von einer Signaturkarte bezogen wird.

Entschlüsselung mit Passwort

Wenn Sie die Entschlüsselung mit einem Passwort auswählen, werden Sie auf der letzten Dialogseite "Entschlüsseln" zur Eingabe eines Passworts aufgefordert.

	**Hinweis**: Bitte beachten Sie, dass dieses Passwort dasselbe sein muss, wie dass das zum Verschlüsseln verwendet wurde.

Entschlüsselung mit privatem Schlüssel

Geben Sie den privaten Schlüssel an, mit dem Sie die Dateien entschlüsseln wollen. Sollten Sie über mehrere Keystores verfügen und verschiedenen Geschäftspartnern unterschiedliche öffentliche Schlüssel geschickt haben, müssen Sie an dieser Stelle wissen, mit welchem öffentlichen Schlüssel die Dateien verschlüsselt wurden, damit Sie den richtigen privaten Schlüssel auswählen können.

-  **Schlüssel aus Datei laden**: Wenn Sie einen privaten Schlüssel aus einer Datei laden wollen, klicken Sie auf dieses Symbol und navigieren Sie an die Stelle im Dateisystem, an der dieser Schlüssel abgelegt ist. Es muss ein Keystore geladen werden, dessen Dateiname mit dem Suffix `.p12` oder `.pfx` endet. Ein Keystore enthält ein Zertifikat und das benötigte Schlüsselpaar für die asymmetrische Ver- und Entschlüsselung. Lesen Sie dazu auch das Kapitel **12.5** über asymmetrische Verschlüsselung.

-  **Signaturkarte**: Diese Auswahl wird nur angezeigt, wenn Sie einen Kartenleser angeschlossen und eine Signaturkarte eingelegt haben. Unter diesem Symbol steht der Name des Kartenlesers, der von der WebEdition erkannt wurde. Sie können bis zu 10 Kartenleser anschließen. Sollten Sie weitere Kartenleser anschließen wollen, lesen Sie zuvor die mitgelieferten Dokumente zu den Systemvoraussetzungen. Auf einer Signaturkarte befindet sich auch ein Verschlüsselungszertifikat. Wählen Sie hier die Signaturkarte aus, damit Sie den darauf enthaltenen privaten Schlüssel zum Entschlüsseln benutzen können.

	**Hinweis**: Sind im Dialogabschnitt "Speicherort des Schlüssels" Symbole von Kartenlesern **ausgegraut**, sind diese **nicht** auswählbar. Wenn Sie eine Signaturkarte benutzen wollen, müssen Sie diese in einen angeschlossenen Kartenleser einlegen. Wenn die Signaturkarte vom Kartenleser eingelesen wurde, ist das Symbol nicht mehr ausgegraut und auswählbar.

Wenn Sie einen Schlüssel ausgewählt haben, wird im darunterliegenden Dialogabschnitt der Schlüssel angezeigt. In einem Keystore oder auf einer Signaturkarte können mehrere Schlüssel enthalten sein. Wenn dies so ist, müssen Sie einen Schlüssel durch Anklicken in der Liste auswählen. Sie dürfen nur einen Schlüssel auswählen.

 Der angezeigte oder ausgewählte Schlüssel gehört zu einem Zertifikat, das Sie über das Lupensymbol anzeigen können. Sie können die Zertifikatsanzeige entweder mit dem OK Button  beenden oder mit dem "Speichern" Button  als Datei abspeichern.

10.3 Zielverzeichnis wählen

Bitte beachten Sie, dass Dialogseiten ganz oder teilweise ausgegraut sein können oder gar nicht angezeigt werden, wenn die dort vorhandenen Einstellungen bereits von Ihrem Diensteanbieter festgelegt wurden.

Sollen verschlüsselte ZIP-Archive im Zielverzeichnis direkt entpackt werden?

- **Ja/Nein**: Sollten Sie eine ZIP-Archivdatei entschlüsseln, können Sie über diese Option steuern, ob diese ZIP-Archivdatei nach dem Entschlüsseln entpackt werden soll. Ist diese Option ausgewählt, wird im Zielverzeichnis für jedes entschlüsselte ZIP-Archiv ein gleichnamiges Unterverzeichnis angelegt und der Inhalt des Archivs darin entpackt.

Zielverzeichnis wählen

Im Zielverzeichnis werden die Dateien abgelegt, nachdem Sie die ausgewählte Funktion ausgeführt haben. Der Dialog bietet Ihnen zwei Optionen. Sie können entweder das Quellverzeichnis nutzen oder ein neues Zielverzeichnis auswählen. Die getroffene Auswahl wird blau umrandet.

- **Quellverzeichnis nutzen**: Diese Einstellung ist die Standardauswahl. Nachdem Sie die ausgewählten Funktionen angewendet haben, werden die Ergebnisdateien in dasselbe Verzeichnis geschrieben, aus dem die jeweilige Originaldatei stammt.
- **Zielverzeichnis wählen**: Bei dieser Auswahl öffnet sich gleichzeitig ein Auswahldialog, über den Sie ein Verzeichnis festlegen können, in das alle Ergebnisdateien geschrieben werden. Der Pfad zum Zielverzeichnis wird danach unter dem Button "Zielverzeichnis wählen" angezeigt.

Lokale Kopie erstellen

Wenn Sie Kopien der entschlüsselten Dateien an einem zusätzlichen Ort speichern möchten, können Sie diesen hier auswählen.

- **Zielverzeichnis wählen**: Wählen Sie über den Button ein Verzeichnis aus, in dem Sie Kopien der Dateien speichern wollen.
- **Zielverzeichnis löschen**: Wählen Sie den Button mit dem Papierkorbsymbol um das ausgewählte Verzeichnis wieder zu löschen. Wenn Sie das Zielverzeichnis gelöscht haben, werden keine lokalen Kopien in das Zielverzeichnis kopiert.

Hinweis: Bitte beachten Sie, dass die hier getroffenen Einstellungen beim nächsten Programmaufruf der WebEdition nicht mehr vorhanden sind.

10.4 Entschlüsseln

Auf dieser letzten Dialogseite der Funktion Entschlüsseln werden die Dateien, die Sie zum Entschlüsseln ausgewählt haben, aufgelistet. Das Entschlüsseln starten Sie mit dem Entschlüsseln-Button unten auf der Seite.

Die Listendarstellung

Die Zeilen in der Listendarstellung haben die folgenden Spalten:

- **Datei**: Zeigt den Namen der Datei an, die Sie zur Entschlüsselung ausgewählt haben. Wenn Sie den Mauszeiger über den Dateinamen legen, wird der vollständige Pfad angezeigt.
- **Status**: Diese Spalte zeigt den Verarbeitungsstatus der Datei an. Diese Meldungen werden angegeben:
  - **Neu**: die Datei wurde noch nicht verarbeitet.
  - **In Arbeit**: die Verarbeitung wird gerade durchgeführt.
  - **Entpackt**: Wenn Sie auf der Dialogseite "Zielverzeichnis wählen" die Option zum Entpacken von Archivdateien angeklickt haben, wird die Archivdatei hier verarbeitet. Dabei entsteht die Archivdatei selbst im Zielverzeichnis und bekommt den Status "Entpackt".
  - **Fertig**: die Verarbeitung ist abgeschlossen.
  - **Fehler**: bei der Verarbeitung ist ein Fehler aufgetreten.
- **Ergebnisdatei**: Das Ergebnis des Entschlüsselns ist die originale Datei. Wenn Sie auf der Dialogseite "Zielverzeichnis wählen" die Option zum Entpacken von Archivdateien angeklickt haben, wird die Archivdatei im Zielverzeichnis entschlüsselt, siehe Status "Entpackt". Nach dem Entschlüsseln wird ein Unterverzeichnis angelegt, das denselben Namen hat, wie die Archivdatei. In dieses Unterverzeichnis wird die Archivdatei entpackt. Nach dem Entpacken wird das neu angelegte Unterverzeichnis in der Listendarstellung mit dem Status "Fertig" angezeigt.

Ergebnisdatei vorhanden

Wenn beim Erstellen der Ergebnisdatei bemerkt wird, dass eine Datei mit gleichem Namen im Zielverzeichnis und/oder im Verzeichnis für lokale Kopien bereits vorhanden ist, wird der Dialog "Zieldatei vorhanden" angezeigt. Sie haben hier die Möglichkeit, eine Auswahl zu treffen.

- **Überschreiben**: Die neue entschlüsselte Datei ersetzt die bereits vorhandene.
- **Umbenennen**: Beim Umbenennen wird der Datei das aktuelle Datum im Dateinamen vorangestellt.
- **Abbrechen**: Sie können die Verarbeitung auch abbrechen.

Sollten Sie mehrere Dateien entschlüsseln, besteht beim Überschreiben oder Umbenennen zusätzlich die Möglichkeit, diese Aktion auf alle nachfolgend zu entschlüsselnden Dateien anzuwenden, deren Ergebnisdateien ebenfalls bereits vorhanden sind. Wählen Sie dazu die Option "Aktion für nachfolgende Dateien automatisch durchführen" im selben Dialog.

Diese Option hat keine Auswirkung, wenn Sie "Abbrechen" wählen. In diesem Fall wird der Dialog bei jeder weiteren, bereits vorhandenen Ergebnisdatei erneut angezeigt. Wird die Verarbeitung abgebrochen, wird dies als Fehler gewertet.

Passwort-basierte Entschlüsselung

Dateien mit der Endung `.enz` sind für gewöhnlich mit einem Passwort verschlüsselt. Bei Dateien mit dieser Endung werden Sie aufgefordert, ein Passwort einzugeben. Dieses Passwort muss dasselbe sein, das zuvor für die Verschlüsselung benutzt wurde.

Ende des Entschlüsselungsprozesses

Wenn der Entschlüsselungsprozess ohne Fehler durchgeführt werden konnte, beendet sich die WebEdition automatisch. Traten ein oder mehrere Fehler auf, wird dies durch ein Dialogfenster angezeigt. Die WebEdition wird dann mit bestätigen dieses Dialoges beendet.

Ihr Dienstanbieter kann festlegen, wie danach verfahren wird. Entweder kehren Sie zur aufrufenden Fachanwendung zurück oder Sie werde auf eine Seite weitergeleitet, die der Dienstanbieter festgelegt hat. Der Dienstanbieter kann auf so einer Seite beispielsweise die Statusmeldungen der WebEdition auflisten. So dass Sie Erfolgs- oder Fehlermeldungen erneut nachlesen können.

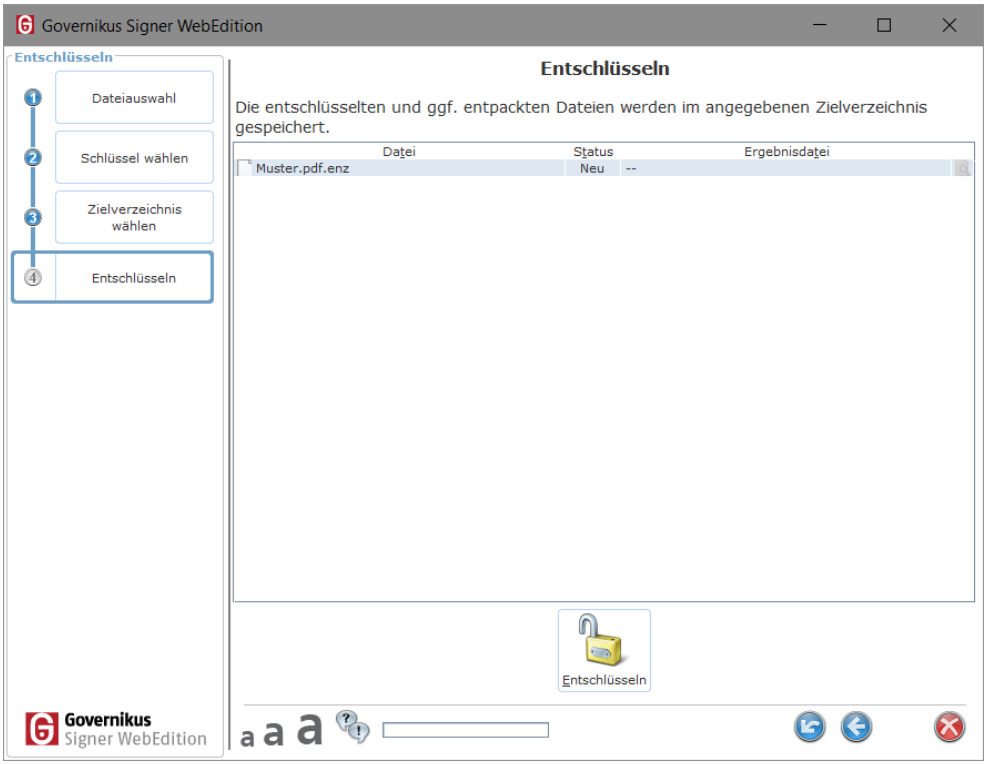


Abbildung 35: Dialogseite "Entschlüsseln"

11 Sicherheit und Datenschutz

Die WebEdition ist eine sichere Anwendung für das Signieren und Siegeln von Dateien. Auf Herstellerseite – der Governikus KG – betreiben wir viel Aufwand, damit jedes neue Release den Ansprüchen der Kunden und den gesetzlichen Anforderungen genügt.

- **Empfehlungen für den Betrieb**: Für den sicheren Betrieb der WebEdition werden besondere Anforderungen an die Software und die Einsatzumgebung gestellt. Dies Anforderungen sind als Empfehlungen formuliert und werden im folgenden Kapitel beschrieben.
- **Privacy by Design**: Bei der Erhebung und Verarbeitung personenbezogener Daten sind durch §3a des Bundesdatenschutzgesetzes Datenvermeidung und Datensparsamkeit vorgegeben. Wie die Governikus KG dies umsetzt ist im Kapitel 11.2 beschrieben.
- **Security by Design**: Die Governikus KG hat Mechanismen etabliert, um die höchstmögliche Sicherheit ihrer Software zu garantieren. Dies ist in Kapitel 11.3 beschrieben.

11.1 Empfehlungen für den Betrieb

Um qualifizierte elektronische Signaturen und Siegel sicher, korrekt und vertrauenswürdig anbringen zu können, sind besondere Anforderungen an die Software selbst und die Einsatzumgebung zu stellen. Eine notwendige hohe Sicherheit gegenüber potenziellen Bedrohungen muss immer komplett sein, d.h. wird immer durch einen "Mix" von Sicherheitsvorkehrungen in der Software selbst und in der Einsatzumgebung komplettiert.

11.1.1 Empfohlene Anforderungen an die Einsatzumgebung

Folgende Empfehlungen bezüglichen der räumlichen und technischen Gegebenheiten bestehen:

- Anbindung an ein Netzwerk:
  - Netzwerkverbindungen sollten so abgesichert werden, dass Angriffe erkannt bzw. unterbunden werden - z. B. durch eine geeignet konfigurierte Firewall und durch die Verwendung geeigneter Anti-Viren-Programme.
- Sicherheit der IT-Plattform und Programme:
  - Von der Hardware, auf der die WebEdition betrieben wird, dürfen keine Angriffe ausgehen. Installierte Software darf nicht böswillig manipuliert oder verändert werden. Maßnahmen gegen Viren oder Trojaner sollten regelmäßig geprüft und aktualisiert werden.
- Schutz vor manuellem Zugriff Unbefugter und Datenaustausch per Datenträger: Folgende Empfehlungen bestehen bezüglich der baulichen, personellen und organisatorischen Anforderungen:

- Unbefugte dürfen keinen Zugriff auf den PC haben, auf dem die WebEdition betrieben wird. Dies sollte ausgeschlossen oder zumindest mit hoher Sicherheit erkennbar sein - beispielsweise durch Sperren des Rechners oder Verschließen des Raumes bei Abwesenheit.
- Beim Übertragen von Daten, die auf Datenträgern vorliegen sollte - z. B. durch die Verwendung geeigneter Anti-Viren-Programme - sichergestellt werden, dass keine Viren oder trojanische Pferde übertragen werden können.

11.1.2 Empfehlungen für den sicheren Betrieb

- Passwörter sollten hinreichend komplex sein (z.B. für die Anmeldung am Betriebssystem), d. h. nutzen Sie
  - keine Trivialpasswörter (z. B. "BBBBBBBB" oder "12345678"),
  - Passwörter mit mindestens einem Zeichen pro Passwort, das kein Buchstabe ist (Sonderzeichen oder Zahl),
  - Passwörter, die mindestens 8 Zeichen lang sind.
- Passwörter müssen geheim gehalten werden: Stellen Sie sicher, dass niemand Ihr Passwort kennt.
- Das persönliche Verzeichnis (Profil-Verzeichnis) des Benutzers, der die WebEdition betreibt, sollte gegen Manipulationen durch Unbefugte geschützt werden - z.B. durch Einschränkung der Zugriffsberechtigung.
- Vor der Installation der Software ist die Integrität des Installationspakets über einen Vergleich eines vor Ort erstellten Hashwerts mit dem durch die Governikus KG veröffentlichten Hashwert zu prüfen.

11.1.3 Technische Anforderungen

Die für den Betrieb der WebEdition unterstützte Hard- und Software ist im Handbuch "Governikus-Signer-WE-Systemanforderungen" beschrieben. Zur Ausstattung für die Erstellung von qualifizierten elektronischen Signaturen und Siegeln zählen die folgenden Karten und Kartenleser:

- Es können qualifizierte elektronische Signaturerstellungseinheiten sowie qualifizierte elektronische Siegeleinheiten verwendet werden, die durch qualifizierte Vertrauensdiensteanbieter aus Deutschland herausgegeben werden und mit denen man eine QES erzeugen kann.
- Seit dem 01.07.2016 gilt in Deutschland die eIDAS-Verordnung, die keine Zertifizierung von geeigneten Chipkartenlesern regelt.

11.1.4 Anforderungen an die Konfiguration

Hinsichtlich der Konfiguration müssen Sie folgende Anforderungen berücksichtigen:

- **Zeitstempelserver**: Für das Anbringen von qualifizierte Zeitstempeln ist ein vertrauenswürdiger Zeitstempelserver einzurichten, der die qualifizierten Zeitstempel über einen Zeitstempel-Anbieter erstellen lässt. Die Verbindungsdaten für einen externen Zeitstempeldienstleister hinterlegt Ihr WebEdition Administrator in der Konfiguration. Ist kein Zeitstempeldienst hinterlegt, ist die entsprechende Auswahl auf der Dialogseite "Optionen" nicht auswählbar. Durch die Konfiguration eines Zeitstempelservers werden keine personenbezogenen Daten verarbeitet.

11.2 Privacy by Design

Datenschutz und Datensicherheit in Governikus Produkten

Bei der Erhebung und Verarbeitung personenbezogener Daten sind durch §3a des Bundesdatenschutzgesetzes Datenvermeidung und Datensparsamkeit vorgegeben. Diese Vorgabe setzen wir in Entwurf und Implementierung (Privacy by Design) und Konfiguration (Privacy by Default) unserer Softwareprodukte um.

11.2.1 Privacy by Design - Produktentwicklung

Vorausplanende Entwicklung und tägliche Tests der Entwicklungsstände helfen, Lücken bei der personenbezogenen Datenverarbeitung zu erkennen und so zu verhindern. Dabei wird der Schutz dieser Daten als Grundeinstellung unserer Produkte verankert und von der Erhebung der Daten bis zur Löschung gesichert. Konkret wird dies durch anerkannte, bewährte und moderne Standards umgesetzt.

Für alle Produkte gilt die **Datentrennung** in personenbezogene Daten und Prozessdaten, das heißt, dass beispielsweise die von den Produkten geschriebenen **Protokolldateien** keine personenbezogenen Daten enthalten und nur für die Überwachung und Fehlersuche eingesetzt werden können.

11.2.2 Privacy by Default - Produktkonfiguration

Die WebEdition signiert Dokumente und ist vom BSI für den Einsatz in der Geheimhaltungsstufe "Verschlusssache nur für den Dienstgebrauch" (VS-NfD) freigegeben und als zugelassen zertifiziert.

Beim Signieren von Dateien werden nach dem Beenden der Verarbeitung keine Daten in der Software gespeichert. Die Konfiguration der WebEdition enthält zu keiner Zeit persönliche Daten. Daten in der Konfiguration werden ausschließlich für die korrekte Ausführung der Software und für die Verarbeitung von Dateien eingetragen.

11.3 Security by Design

Die Governikus KG hat Mechanismen etabliert, um die höchstmögliche Sicherheit ihrer Software zu garantieren.

11.3.1Überwachung von Drittanbieter-Produkten

In der WebEdition sind auch Programme von Drittanbietern enthalten, sogenannte 3rd Party Libs. Die in der WebEdition enthaltenen Programme von Drittanbietern werden im Dokument "Governikus-Signer-WE Nutzungsbedingungen" aufgelistet. In allen Entwicklungs-Teams der Governikus KG sind automatische Überwachungsmechanismen etabliert, die die Aktualität der 3rd Party Libs ständig überwachen. Wird eine neue Version gemeldet, wird von einem verantwortlichen Entwickler geprüft, ob die neuere Version in unseren Produkten ausgetauscht werden soll. Diese Prüfung durch einen Entwickler ist notwendig, da auch Beta-Versionen als neue Versionen gemeldet werden. Beta 3rd Party Libs sind in der Testphase und werden daher nicht in unsere Produkte eingebaut. Finale neue 3rd Party Libs werden getestet und danach übernommen.

11.3.2Geschützte Produktionsumgebung

Governikus Produkte werden in besonders geschützten Räumlichkeiten entwickelt. Der Zugang ist mit Transpondern und Alarmanlage gesichert. Der räumliche Schutz und der Schutz der besonders gesicherten Produktions-Infrastruktur ist im Governikus Sicherheitskonzept beschrieben, auf dessen Grundlage die Evaluierung nach Common Criteria erfolgt. Dabei wird die Vertrauenswürdigkeitsanforderung "Development Security (ALC_DVS.1)" aus der Vertrauenswürdigkeitsklasse "Life-Cycle Support (ALC)" geprüft. Darüber hinaus ergänzt dieses Konzept das Datenschutzkonzept.

11.3.3 Bewertung von Gefährdungen

Als ständiger Prozess findet eine technische Bewertung von Gefährdungen durch unsere Technology Coaches statt. Dies betrifft sowohl die in Governikus Produkten eingesetzten Technologien und die verwendeten Drittanbieterprodukte, als auch die Sicherheit und Verfügbarkeit der Infrastruktur. Dabei werden alle einschlägigen Quellen überwacht und bewertet, die über diese Produkte berichten. Trifft eine Sicherheits- oder Verfügbarkeits-relevante Gefährdung für uns zu, wird über bewährte Verfahren, wie Software-Aktualisierung, Mailings oder Patches, sofort reagiert. So werden die Sicherheit der ausgelieferten Governikus Produkte und damit die Sicherheit der personenbezogenen Datenverarbeitung gewährleistet und dokumentiert.

11.4 DSGVO und WebEdition

Einleitung

Die DSGVO regelt den Schutz personenbezogener Daten und die Rechte der Bürger an ihren personenbezogenen Daten. Die Software WebEdition der Governikus KG ist Teil der Auslieferung der WebEdition. Die Software WebEdition verarbeitet zum Teil auch personenbezogene Daten. Die folgende Beschreibung liefert die entsprechenden Aussagen zu den Funktionen der WebEdition.

Download und Installation

Die Software WebEdition der Governikus KG ist Teil der Auslieferung der WebEdition. Beim Download der Software ist die Kommunikation zwischen dem Rechner des Benutzers und dem Download-Server der Governikus KG SSL-verschlüsselt. Die IP-Adresse des Benutzers wird auf dem Download-Server im Server-Protokoll anonymisiert gespeichert, indem die letzten beiden der vier IP-Blöcke jeweils den Wert 0 erhalten. Damit ist eine Rückverfolgung des Benutzers nicht mehr möglich. In den Installationspaketen der WebEdition sind keine personenbezogenen Daten enthalten.

Zertifikate mit personenbezogenen Daten

In der WebEdition können Zertifikate eingesetzt werden, die personenbezogene Daten enthalten. In Zertifikaten kann der Name des Zertifikatsinhabers (Common Name = CN) stehen. Es können weitere personenbezogene Daten in Zertifikaten enthalten sein, wenn dies der Aussteller oder Zertifikatsinhaber vorgegeben hat. Dies gilt auch für Pseudonyme in Zertifikaten, da auch hier einen Personenbezug hergestellt werden kann.

Das Einverständnis des Betroffenen bei der Verarbeitung dieser personenbezogenen Daten wird implizit vorausgesetzt, da sonst das Signieren, Ver- oder Entschlüsseln von Dateien nicht möglich ist. Die Verantwortung für das datenschutzkonforme Ausstellen und Veröffentlichen von Zertifikaten liegt bei der Zertifizierungsstelle, also dem Zertifizierungs-dienstanbieter.

Konfiguration der WebEdition

Die Konfiguration der WebEdition nimmt ein Administrator in einem Webserver vor, beispielsweise Tomcat. Ein Anwender hat bei der Benutzung der WebEdition keinen Einfluss auf die Konfiguration, da diese vom Administrator vorgegeben ist. Die Konfiguration enthält keine personenbezogenen Daten. Hat der Administrator den Aufruf des Dialogs "Einstellungen" für den Benutzer freigeschaltet, kann der Benutzer für die Dauer eines Aufrufs personenbezogene Daten in der Registerkarte PDF eintragen. Diese werden nur für einen Aufruf vorgehalten und werden nach Beenden verworfen.

Log-Dateien

Die WebEdition wird in einem Webserver, beispielsweise Tomcat, deployed. Die Ereignisse der Funktionen Signieren, Verschlüsseln und Entschlüsseln werden in gemeinsame Protokolldateien geschrieben. In diesen Log-Dateien sind keine personenbezogenen Daten enthalten, es werden keine Zertifikatsdaten in den Log-Dateien protokolliert.

Datensparsamkeit

Das Gebot der Datensparsamkeit ist durchgängig berücksichtigt. Es werden grundsätzlich nur die Daten verarbeitet, die für die Funktionen der WebEdition benötigt werden. Es werden keine Daten erhoben.

Schutz der Daten vor unbefugtem Zugriff durch Dritte

Der Ort der Speicherung von signierten, ver- oder entschlüsselten Dateien liegt in der Verantwortung des Benutzers der WebEdition. Folgt der Benutzer den Empfehlungen für den Betrieb, die im Kapitel 11 beschreiben sind, ist ein angemessener Schutz gewährleistet. Die Umsetzung der Empfehlungen liegt in der Verantwortung des Benutzers und ist dem Einfluss der Governikus KG entzogen.

11.5 Gesetzliche Grundlagen

EU DSGVO

Die EU-Datenschutz-Grundverordnung (EU DSGVO) ist Grundlage für Sicherheit und Datenschutz bei der Governikus KG, dort Art. 25 sowie der Erwägungsgrund 78, Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

BDSG

Das neue Bundesdatenschutzgesetz (BDSG-neu), basierend auf dem DSAnpUG-EU, dort § 71 (DSAnpUG-EU = Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU)).

DSAnpUG-EU-Entwurf

Die amtliche Begründung zu DSAnpUG-EU-Entwurf zu dieser Vorschrift.

12 Erläuterungen

Im Folgenden werden die Begriffe und Hintergründe erläutert, die im Kontext der WebEdition wichtig sind. Die Definitionen und Erklärungen in diesem Kapitel erheben keinen Anspruch auf Vollständigkeit und ersetzen keine rechtliche Beratung.

Die Erklärungen in diesem Kapitel sind alphabetisch geordnet, da es wegen der unterschiedlichen Benutzungsszenarien der WebEdition keine immer zutreffende, logische Reihenfolge geben kann.

12.1 Authentifizierung und Authentisierung

Diese beiden Begriffe bedeuten im Deutschen unterschiedliche Vorgänge. Im Englischen gibt es dafür nur einen Begriff - Authentication.

Authentifizierung

Authentifizierung ist der Nachweis der Berechtigung. So ist es beispielsweise üblich, sich gegenüber geschützten Rechnersystemen mit Login und Passwort zu authentifizieren.

Authentisierung

Authentisierung ist der Nachweis der Identität, beispielsweise mit einem Pass gegenüber Behörden. Bei einer Datei, die elektronisch mit einer Signaturkarte signiert wurde, ist so nachweisbar, wer diese Signatur angebracht hat.

12.2 Elektronische Signatur

Eine elektronische Signatur bezieht sich immer auf genau eine Datei. Sie kann in der Datei selbst enthalten sein oder als zusätzliche Datei erstellt werden. Die elektronische Signatur für Dateien ist mit einem Siegel vergleichbar, mit dem die Unversehrtheit und Authentizität von Dingen oder Behältern beglaubigt wird. Bei elektronischen Signaturen werden die folgenden vier Typen unterschieden, von denen nur die beiden letzten rechtlich einer eigenhändigen Unterschrift weitestgehend gleichgestellt sind.

- Einfache elektronische Signaturen (beispielsweise eine Unterschrift, die gescannt und als Bilddatei in eine Datei eingefügt wurde)
- Fortgeschrittene elektronische Signaturen (beispielsweise erstellt mit einem Software-zertifikat)
- Qualifizierte elektronische Signaturen (erstellt mit einer Signaturkarte)
- Qualifizierte elektronische Signaturen mit Anbieter-Akkreditierung (erstellt mit einer Signaturkarte)

Authentizität und Integrität

Ziel der elektronischen Signatur ist es, die Authentizität und Integrität von Daten zu erreichen. Nachdem Sie eine Datei signiert haben, ist es möglich, festzustellen, ob diese Datei wirklich von Ihnen signiert wurde (Authentizität) und ob sie seit dem Anbringen der Signatur verändert wurde (Integrität).

Wie entsteht eine qualifizierte elektronische Signatur?

Eine elektronische Signatur entsteht in drei Schritten. Im ersten Schritt wird für die Datei, die signiert werden soll, ein Hashwert errechnet, im zweiten Schritt wird der Hashwert verschlüsselt und im dritten wird das Zertifikat hinzugefügt.

1. Berechnung des Hashwerts

Für eine elektronische Signatur wird zunächst eine Funktion angewendet, die für eine Datei einen eindeutigen Wert erzeugt. Die Funktion wird Hash-Funktion genannt und der Wert Hashwert. Ein Hashwert benötigt deutlich weniger Speicherplatz als die Datei, aus der er erzeugt wurde. Beispiel für einen Hashwert:

```
0D9C3ECDFBE036E1750DE82A7863F1E6B6AC336B
```

Ein Hashwert ist für jede Datei einmalig. Wenn für eine Datei immer dieselbe Funktion zur Hashwert-Erzeugung benutzt wird, dann kommt bei derselben Datei auch immer derselbe Hashwert heraus. Wird die Datei verändert, entsteht ein anderer Hashwert. Mit diesem Hashwert kann also die **Integrität** der Datei nachgewiesen werden. Solange bei der Hashwert-Berechnung immer derselbe Wert herauskommt, wurde die Datei nicht verändert.

2. Verschlüsselung des Hashwerts

Für die Verschlüsselung des Hashwerts wird ein sogenanntes asymmetrisches Schlüsselpaar benutzt. Es besteht aus einem privaten (geheimen) und einem öffentlichen Schlüssel. Der private Schlüssel ist nur auf der Signaturkarte enthalten und kann von dort nicht entfernt werden. Der öffentliche Schlüssel kann jedem zugänglich gemacht werden. Mit dem privaten Schlüssel wird der Hashwert verschlüsselt. Dazu wird vom Programm, also von der WebEdition, der Hashwert der Datei errechnet. Dieser wird dann an die Signaturkarte übergeben. Innerhalb der Signaturkarte wird dieser Hashwert verschlüsselt und danach wird der verschlüsselte Hashwert an das Programm zurückgegeben. Um den Missbrauch einer Signaturkarte zu verhindern, wird vor dem Verschlüsseln mit dem privaten Schlüssel die persönliche Identifikationsnummer (PIN) abgefragt. Erst bei korrekter PIN-Eingabe wird verschlüsselt.

3.Hinzufügen des Zertifikats

Nach der Rückgabe des verschlüsselten Hashwerts an das Programm wird das Zertifikat von der Signaturkarte als Kopie dem verschlüsselten Hashwert hinzugefügt. Es enthält unter anderem den Namen des Signaturkarteninhabers, den öffentlichen Schlüssel und die Zertifizierungsstelle, die die Signaturkarte ausgestellt hat. Zudem wird der Verschlüsselungszeitpunkt hinzugefügt.

Signierte Datei

Die oben erklärten Bestandteile - verschlüsselter Hashwert, Verschlüsselungszeitpunkt und Zertifikat mit öffentlichem Schlüssel - bilden die elektronische Signatur. Die elektronische Signatur zu einer Datei kann entweder in der signierten Datei selbst enthalten sein, was z. B. bei PDF-Dokumenten möglich ist. Oder andersherum kann die Signatur auch die signierte Datei beinhalten. Diese Signatur heißt dann "enveloped". Ist die Signatur in einer Extradatei enthalten, dann heißt sie "detached". Das Zertifikat kann bis zur Zertifizierungsstelle nachvollzogen werden. Die Zertifizierungsstelle bestätigt auf Anfrage die Identität, womit die Authentizität nachgewiesen werden kann.

Achtung: Der Inhalt einer Datei, die "nur" elektronisch signiert wurde, also nicht verschlüsselt ist, kann durch Dritte angeschaut werden. Mit der elektronischen Signatur können Authentizität und Integrität bewiesen werden, aber ohne Verschlüsselung ist keine Geheimhaltung möglich.

12.3 Signaturkarte

Eine Signaturkarte hat üblicherweise das Format einer Scheckkarte und enthält einen Chip. Dieser Chip enthält üblicherweise drei Zertifikate, es können auch mehr sein.

Zertifikate

Jedes Zertifikat enthält unter anderem Informationen über den Inhaber (Name, Vorname), den Gültigkeitszeitraum (Startdatum und Uhrzeit bis Enddatum und Uhrzeit), den Herausgeber (beispielsweise TeleSec der T-Systems), einen Fingerprint (dient zum schnellen Identifizieren des öffentlichen Schlüssels eines Zertifikats) und die Schlüsselverwendung.

Die drei verschiedenen Zertifikate haben unter anderem eine eigene Seriennummer, einen eigenen Fingerprint und unterschiedliche Schlüsselverwendungen. Die drei üblichen Schlüsselverwendungen sind:

- **keyEncipherment**, **dataEncipherment**: Ein Zertifikat mit dieser Schlüsselverwendung wird dazu benutzt, Dateien zu ver- oder entschlüsseln.
- **nonRepudiation**: Beim Signieren einer Datei wird dieses Zertifikat verwendet. Dabei entsteht die Elektronische Signatur.
- **digitalSignature**: Dieses Zertifikat wird verwendet, wenn ein Inhaber seine Signaturkarte dazu benutzt, sich zu authentisieren.

12.4 Verifizieren

Das Verifizieren ist ein Vorgang, bei dem eine elektronisch signierte Datei auf Authentizität und Integrität überprüft wird. Dieser Dienst wird vom Governikus Verification Service angeboten. Mit dem öffentlichen Schlüssel, der üblicherweise im mitgelieferten Zertifikat der elektronischen Signatur enthalten ist, kann der Hashwert entschlüsselt werden. Nach der Neuberechnung des Hashwerts kann dieser mit dem entschlüsselten Hashwert verglichen werden. Sind diese gleich, ist die Integrität des signierten Dokuments nachgewiesen. Zum Nachweis der Authentizität, also der Identität desjenigen, der behauptet, die Datei signiert zu haben, wird das Zertifikat zur Online-Prüfung an die Zertifizierungsstelle geschickt.

Zertifikatsprüfung

Die Zertifizierungsstelle überprüft das Zertifikat auf Echtheit und Gültigkeit. Mit Gültigkeit ist in diesem Kontext nicht der Gültigkeitszeitraum des Zertifikats gemeint, denn dieser lässt sich aus den Zertifikatsdaten herauslesen. Es geht hier vielmehr darum, dass die Gültigkeit eines Zertifikats bereits vor Ablauf des angegebenen Gültigkeitszeitraums zurückgezogen werden kann, wenn der Inhaber beispielsweise seine Signaturkarte als verloren meldet, oder befürchtet, dass Dritte in den Besitz der Karte und der PIN gelangt sind.

12.5 Verschlüsselung

Bei der Verschlüsselung wird eine Datei, die zuvor beispielsweise einen lesbaren Inhalt (Texte) oder einen verständlich darstellbaren Inhalt (Bilder) hatte, in eine nicht verständliche Repräsentation überführt. Dies kann auch mit anderen Dateien wie beispielsweise Programmdateien durchgeführt werden, die nach der Verschlüsselung nicht mehr ausführbar sind. Mit der Verschlüsselung wird erreicht, dass Dritte keinen Zugriff auf Inhalt oder Funktion einer Datei haben. Für die Rückführung in die Ausgangsrepräsentation muss die Datei entschlüsselt werden. Die Verfahren zur Verschlüsselung einer Datei sind entweder asymmetrisch oder symmetrisch.

Asymmetrische Verschlüsselung

Bei der asymmetrischen Verschlüsselung wird ein Schlüsselpaar benötigt. Es besteht aus einem privaten, geheimen und einem öffentlichen Schlüssel. Der private Schlüssel wird nie herausgegeben, den öffentlichen Schlüssel erhalten alle Geschäftspartner. Die Geschäftspartner tauschen also untereinander ihre öffentlichen Schlüssel aus. Soll nun eine Datei vor der Übertragung verschlüsselt werden, so wird sie mit dem öffentlichen Schlüssel des Geschäftspartners verschlüsselt, an den die Datei gesendet werden soll. Nur dieser Empfänger ist in der Lage, mit seinem privaten, geheimen Schlüssel die Datei wieder zu entschlüsseln.

- **Vorteil**: da nur der Empfänger mit dem privaten Schlüssel Dateien entschlüsseln kann, kann der öffentliche Schlüssel gefahrlos an die Empfänger geschickt werden.
- **Nachteil**: Die asymmetrischen Verschlüsselungsverfahren sind deutlich zeitintensiver, da das Verfahren (der Algorithmus) aufwendiger ist.

Symmetrische Verschlüsselung

Bei der symmetrischen Verschlüsselung wird mit einem einzigen Schlüssel verschlüsselt und entschlüsselt.

- **Vorteil**: Dieses Verfahren ist sehr viel schneller als das asymmetrische Verfahren.
- **Nachteil**: Wenn der symmetrische Schlüssel verschickt wird und dabei abgefangen wird, kann jeder die damit verschlüsselte Nachricht entschlüsseln und beispielsweise verändern und erneut verschlüsseln.

Bei der Verschlüsselung mit Passwort wird die symmetrische Verschlüsselung angewendet. Der zum Ver- und Entschlüsseln benötigte Schlüssel ist das verwendete Passwort.

Hybrides Verschlüsselungsverfahren

Der vom der WebEdition zur Ver- und Entschlüsselung mit Zertifikat verwendete Standard beinhaltet beide Verfahren. Die zu verschlüsselnde Datei wird zunächst mit der schnellen symmetrischen Verschlüsselung verschlüsselt. Den dafür notwendigen symmetrischen Schlüssel erstellt die WebEdition selbstständig. Für jede zu verschlüsselnde Datei wird ein neuer Schlüssel generiert. Dieser symmetrische Schlüssel wird wiederum mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und der symmetrische Schlüssel der verschlüsselten Datei beigefügt. Der Empfänger kommt mit seinem privaten Schlüssel und seiner PIN an den symmetrischen Schlüssel und kann somit die Datei entschlüsseln. Soll eine Datei durch mehrere Empfänger entschlüsselt werden können, wird einfach der symmetrische Schlüssel mehrfach, jeweils mit den verschiedenen öffentlichen Schlüsseln der Empfänger verschlüsselt und hinzugefügt. Als Benutzer merken Sie von diesem zweistufigen Verfahren nichts.

12.6 Zeitstempel

In einer elektronischen Signatur ist normalerweise auch ein Signaturzeitpunkt enthalten. Als Zeitangabe wird durch die Signatursoftware die lokale Systemzeit verwendet. Da diese Zeit jedoch beliebig durch den Benutzer eingestellt werden kann, ist dieser Signaturzeitpunkt nicht vertrauenswürdig.

12.7 Zertifizierungsstelle

Ausgabe von Signaturkarten

Eine Zertifizierungsstelle (englisch Certificate Authority, CA) gibt Signaturkarten heraus. Dabei muss beim Antrag einer Signaturkarte die Identität nachgewiesen werden, beispielsweise mit dem Postident-Verfahren. Die Signaturkarte wird dann an den Antragsteller ausgegeben und es muss ein Freischaltungsprozess durchgeführt werden. Danach ist die Signaturkarte für den angegebenen Zeitraum gültig. Beim Verifizieren von elektronischen Signaturen bestätigt die herausgebende Zertifizierungsstelle die Authentizität desjenigen, der die Signatur angebracht hat.

13 Erste Hilfe

In diesem Kapitel finden Sie Hinweise und Lösungsmöglichkeiten für den Fall, dass es bei der Verwendung der WebEdition zu Problemen kommen sollte.

Signaturkarte kann nicht ausgewählt werden

- **Symptom**: Unter "Speicherort des Schlüssels" ist zwar das Symbol des Kartenlesers vorhanden, es ist aber nur grau dargestellt und kann nicht ausgewählt werden.
- **Mögliche Ursachen**:
  - Es ist keine Signaturkarte eingelegt oder die Signaturkarte ist nicht korrekt eingelegt. Bitte prüfen Sie, ob die Signaturkarte korrekt in den Kartenleser eingelegt ist.
  - Der Kartenleser wird von einer anderen Anwendung blockiert. Bitte prüfen Sie, ob ein anderes Programm auf Ihrem Rechner läuft, dass auf den Kartenleser zugreift und beenden Sie dieses gegebenenfalls.
  - Sie verwenden eine Signaturkarte mit Pseudonym.
  - Zeigen Sie mit dem Mauszeiger auf das ausgegraute Kartenlesersymbol. Es wird ein Hinweistext mit Verweis auf die mögliche Ursache angezeigt.

Ein neu angeschlossener Karteleser steht nicht zur Auswahl

- **Symptom**: Ein Kartenleser wurde angeschlossen. Er wird jedoch nicht unter "Speicherort des Schlüssels" aufgelistet.
- **Mögliche Ursachen**:
  - Die WebEdition prüft nur beim Programmstart, welche Kartenleser verfügbar sind. Nachträglich angeschlossene Kartenleser werden nicht automatisch erkannt. Bitte führen Sie in diesem Fall die Funktion "Karten neu einlesen" aus.
  - Der Kartenleser wird durch die WebEdition nicht unterstützt. Prüfen Sie bitte anhand des beiliegenden Dokumentes "Systemanforderungen", ob Ihr Kartenleser unterstützt wird.
  - Die Treiber-Software für den Kartenleser ist nicht oder nicht korrekt installiert. Prüfen Sie bitte anhand des beiliegenden Dokumentes "Systemanforderungen", ob die von Ihnen verwendete Treiber-Software der unterstützten Version entspricht.

Fehlermeldung "Die Datei wurde verändert"

- **Symptom**: Beim Versuch eine Datei einzusehen, wird lediglich der Warnhinweis angezeigt, dass die Datei verändert wurde.
- **Ursache**: Die WebEdition stellt sicher, dass eine Datei, die Sie sich bereits angesehen haben, vor dem Signieren nicht unbemerkt verändert werden kann. Prüfen Sie bitte in diesem Fall erneut den Inhalt der zu signierenden Datei durch Öffnen und Einsehen der Datei. Achten Sie darauf, dass das verwendete Anzeigeprogramm die Dateien

nicht unbemerkt verändert, z.B., dass die Datei beim Schließen des Anzeigeprogramms nicht automatisch gespeichert wird.

Anwendung schließt sich nicht

- **Symptom**: Nach Beendigung des Signaturvorgangs wird zwar die Benutzeroberfläche zur Signaturerstellung geschlossen, die Anwendung bleibt jedoch geöffnet.
- **Ursache**: Dieses Verhalten kann bei Verwendung des Browsers Firefox auftreten, wenn JavaScript deaktiviert ist. Aktivieren Sie bitte im Einstellungsdialog des Browsers die Ausführung von JavaScript.