GOVERNIKUS


GOVERNIKUS
DATA BOREUM®
Web Edition

# Anwendungshandbuch

## Governikus DATA Boreum WebEdition

Governikus DATA Boreum WebEdition, Release 10.9.0

**Dokumentenversion: 10.9.0_0**

# Inhaltsverzeichnis

# 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.

# 1 Einleitung

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

**Hinweis**: Im Folgenden wird die **Governikus DATA Boreum 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.

## 1.1 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.

## 1.2 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.

## 1.3 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.

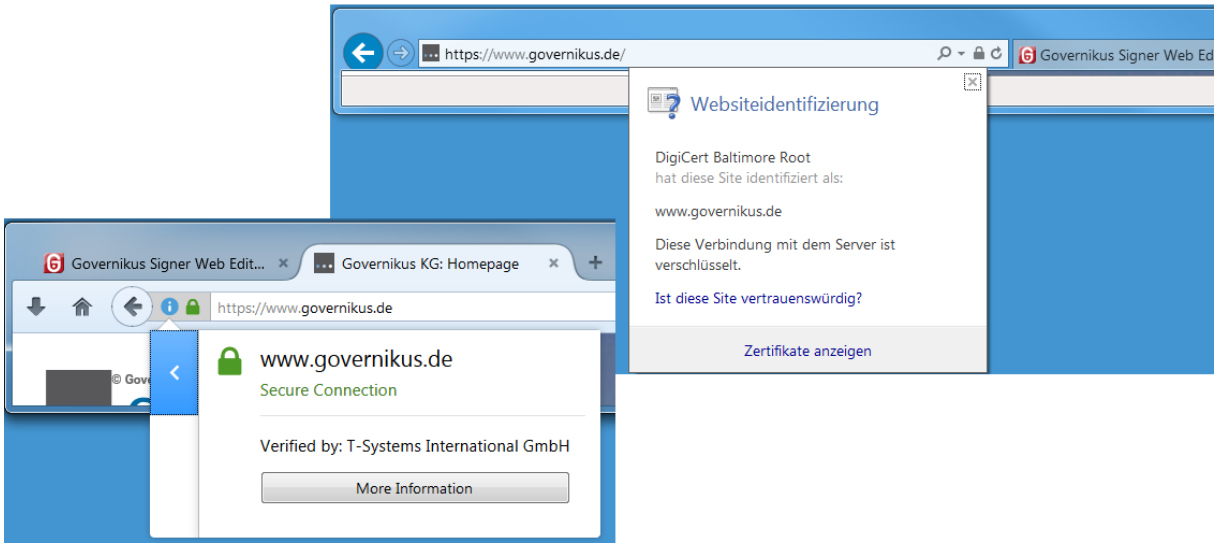


Abbildung 1: Zertifikatsinformationen am Beispiel Firefox und Internet Explorer

# 2 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-DATA-Boreum-WE_Systemanforderungen.pdf`.

### Java Runtime Environment

Die Auslieferung enthält ein Java Runtime Environment, welches ausschließlich für die Nutzung der WebEdition verwendet wird. Es werden keine weiteren JRE-Installationen auf dem Nutzer-PC benötigt.

## 2.1 Unterstützte Betriebssysteme

### Unterstützte Betriebssysteme

Die WebEdition kann auf den folgenden Betriebssystemen eingesetzt werden:

- **Windows**: 10 und 11

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

## 2.2 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-DATA-Boreum-WE_ Systemanforderungen.pdf.`

### Proxy

Die WebEdition funktioniert unabhängig von einem 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. Wenn ein Proxy eine Authentisierung fordert, dann muss der Nutzer die Authentisierungsdaten zur Laufzeit der Anwendung einmal eingeben. Die WebEdition speichert keine Authentisierungsdaten.

## 2.3 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 in Ihrem temporären Verzeichnis. Beispiel für Windows:

`C:\Users\<Ihr-Anmeldename>\AppData\Local\Temp\Governikus KG\DATA Boreum`

`(Aufruf bspw. über: \%temp%\Governikus KG\GovernikusBoreumWebEdition)`

# 3 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 ein Fachverfahren/ein Webportal gestartet. |

### Aufruf des Installers

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

`GovDATABoreumWebEdition_<Versionsnummer>.msi`

### Start des Setup Assistenten

Klicken Sie auf "Weiter"

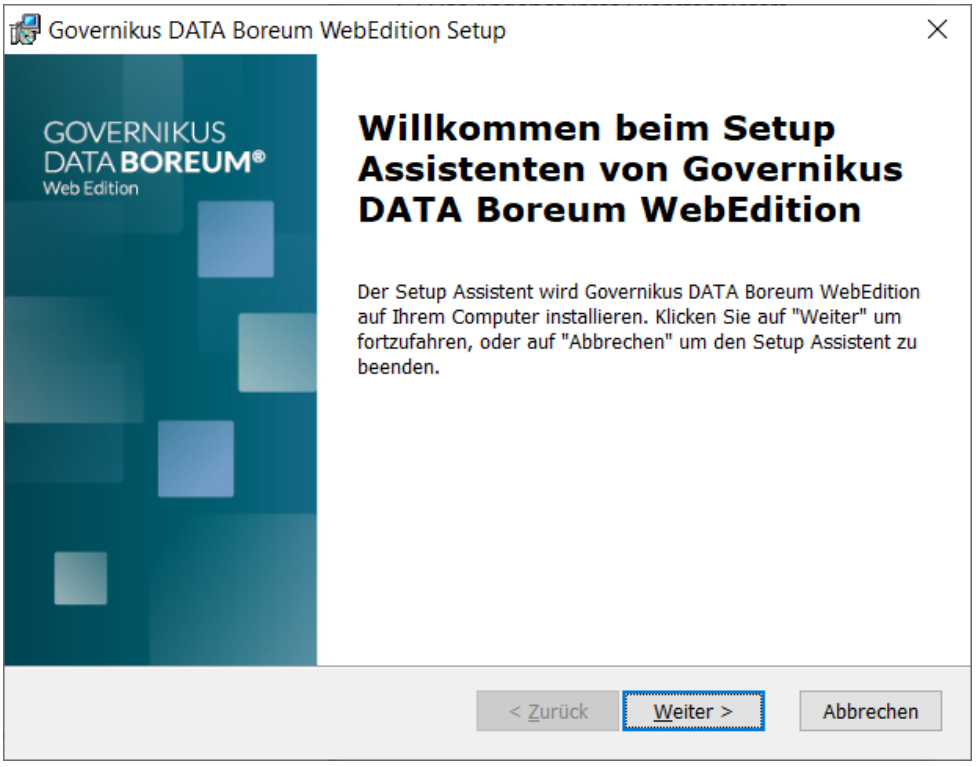


Abbildung 2: Start des Setup Assistenten

### Lizenzvereinbarung

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

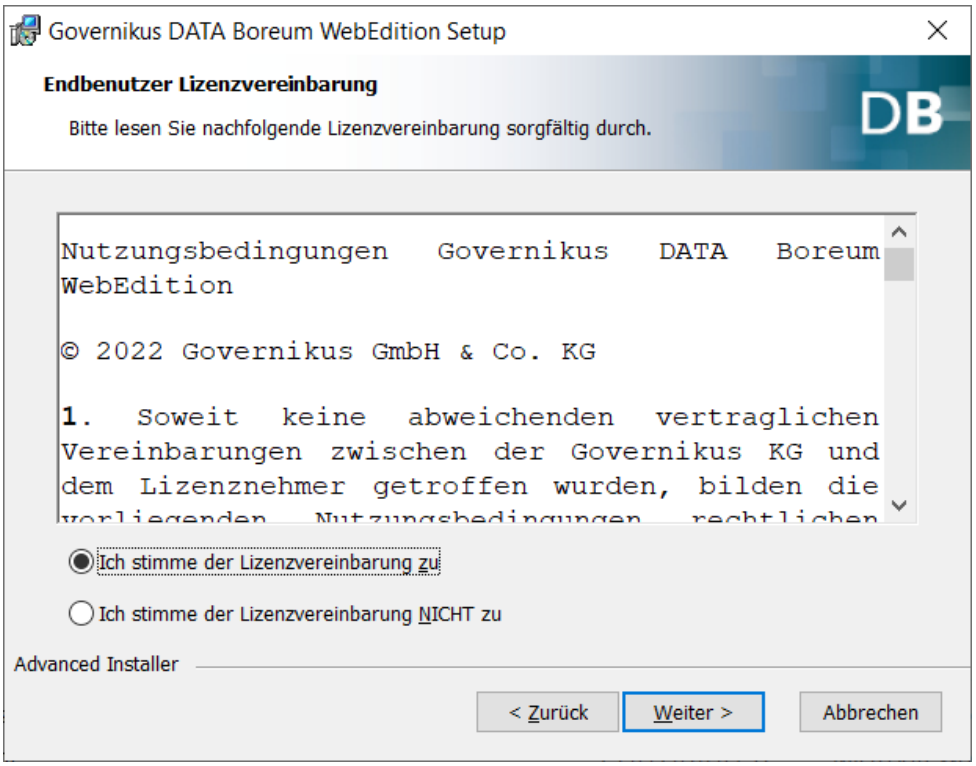


Abbildung 3: Dialogseite mit Lizenzvereinbarung

## Installationsverzeichnis wählen

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

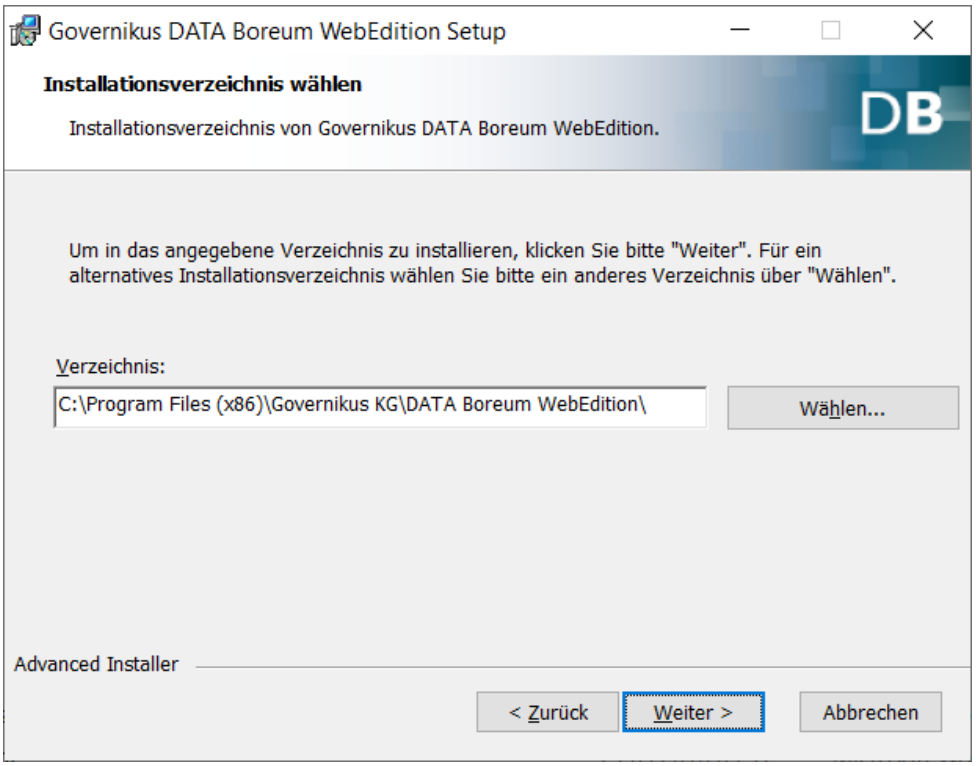


Abbildung 4: Dialogseite Installationsverzeichnis wählen

### Installation bestätigen

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

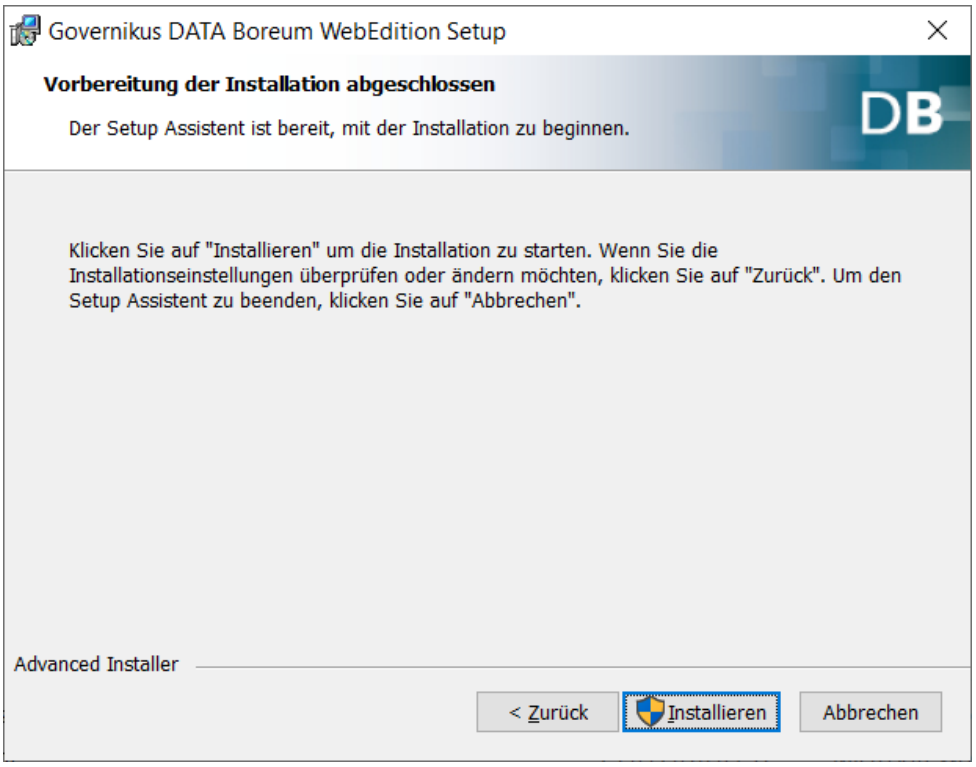


Abbildung 5: Dialogseite Installation bestätigen

### 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.

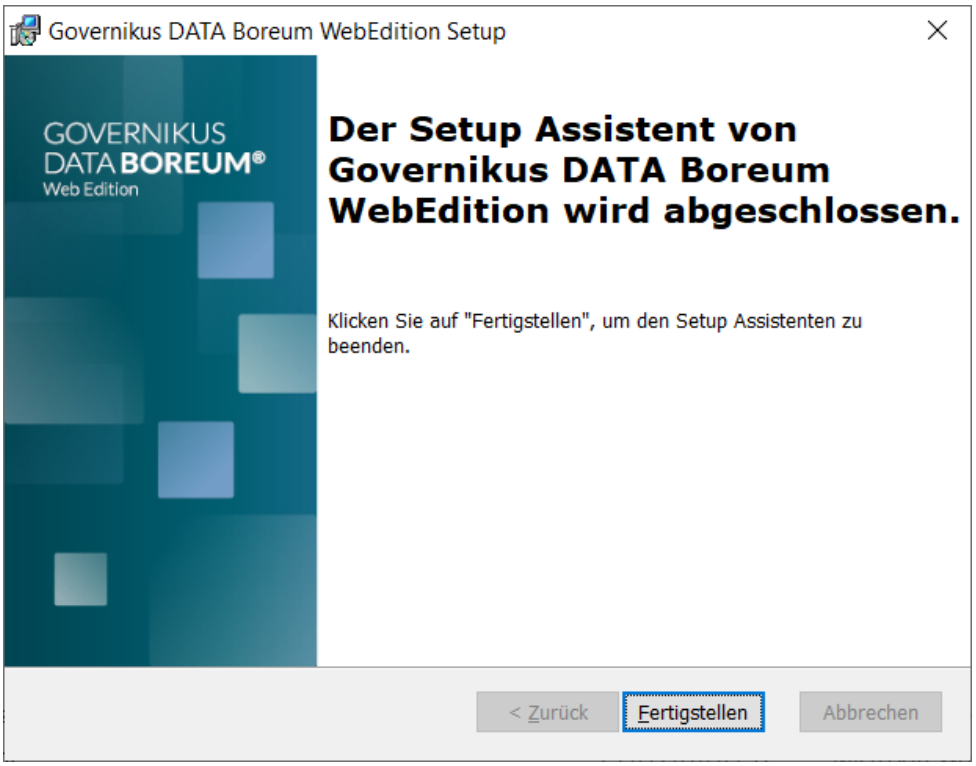


Abbildung 6: Dialogseite Fertigstellen

# 4 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.

## 4.1 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 Anwendungsoberfläche. 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 Anwendungsoberfläche

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

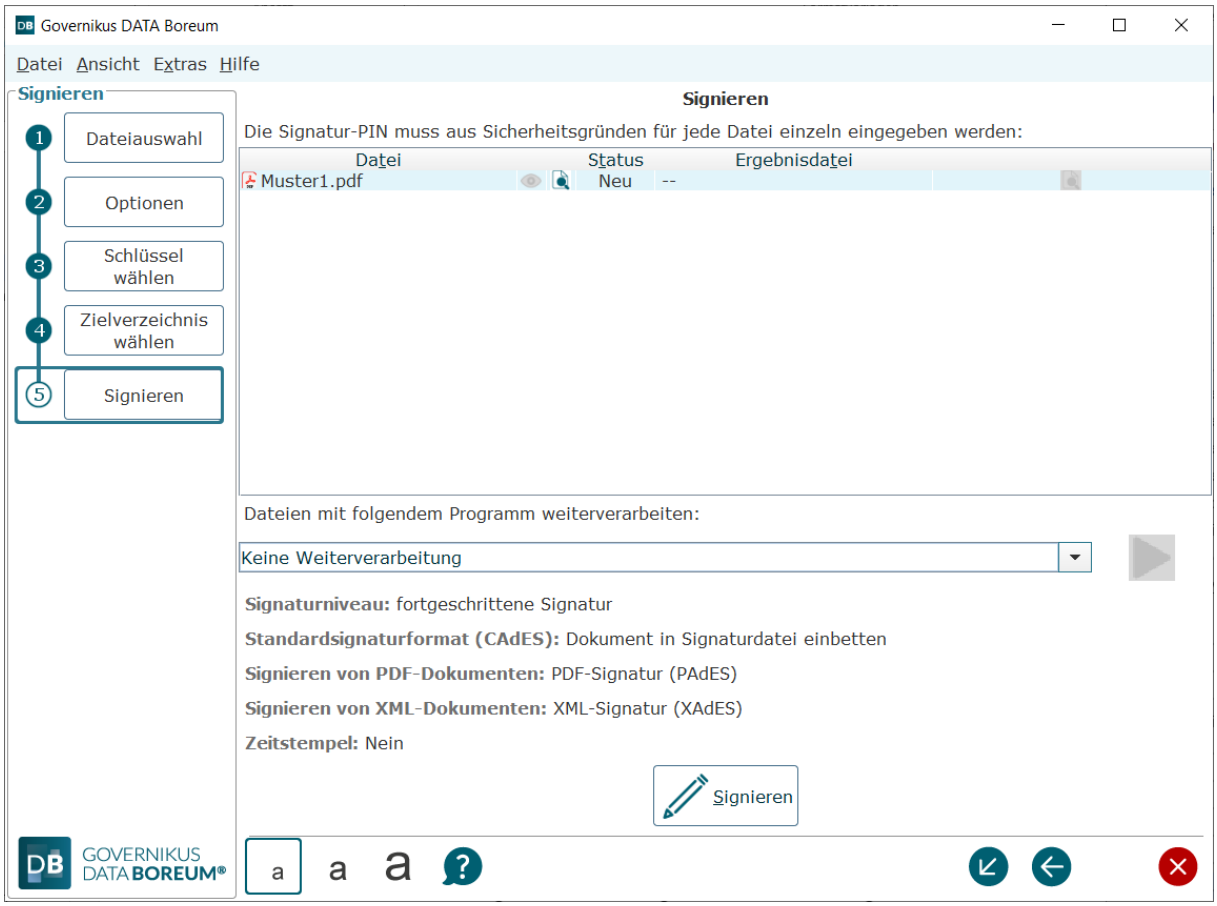


Abbildung 7: WebEdition mit Dialogseite "Signieren"

## 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 herunterlädt (zu Hashwerten lesen Sie bitte auch Kapitel 10.2). 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:

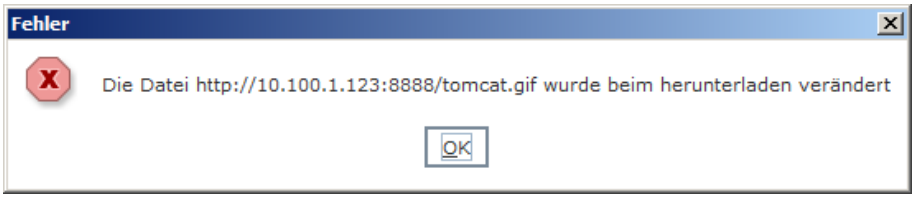


Abbildung 8: Beispielhafter Warndialog bei veränderter Datei

| | |
|---|---|
|  | **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! |

## 4.2 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 Anwendungsoberfläche. 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 Anwendungsoberfläche

Die folgende Abbildung zeigt die Anwendungsoberfläche 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.

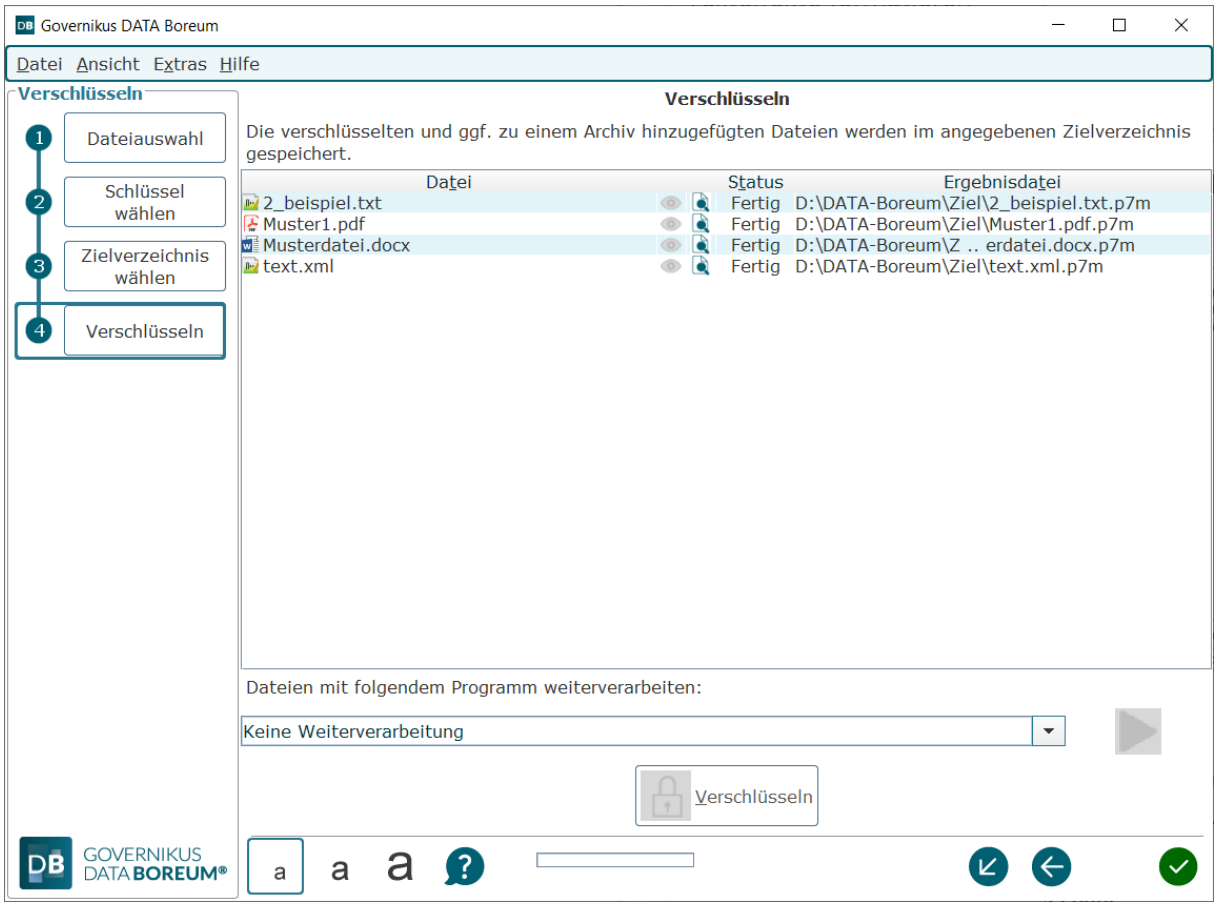


Abbildung 9: Anwendungsoberfläche der WebEdition mit der Dialogseite "Verschlüsseln"

## 4.3 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.

# 5 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.

## 5.1 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 in die WebEdition 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 5.6 erklärt.

## 5.2 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.

### 5.2.1 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 Validierungsanwendung eingesehen oder extrahiert werden, beispielsweise durch die Funktion "Validieren" der WebEdition.

- **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 validiert werden, müssen beispielsweise der Funktion "Validieren" der WebEdition beide Dateien übergeben werden.

| | |
|---|---|
|  | **Hinweis**: Eine Datei (bspw. Musterschreiben.docx) kann von beliebig vielen Personen nacheinander detached signiert werden. Die Signaturen werden alle in einer Signaturdatei (bspw. Musterschreiben.docx.p7s) aufgenommen, vorausgesetzt, die Signaturdatei liegt im selben Ordner wie die Inhaltsdatei. Liegt die Signaturdatei in einem anderen Ordner als die Inhaltsdatei, die zum Signieren ausgewählt wird, wird mit dem Signaturvorgang eine neue Signaturdatei erstellt. |

### 5.2.2 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.
  - **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.
  - **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.

**Hinweis**: Wenn Sie hier einen Grund und/oder Ort der Unterschrift eingeben, werden diese Angaben bei Auswahl eines sichtbaren Signaturfeldes angezeigt. Für Unsichtbare Signaturen werden diese Angaben ebenfalls in die Unterschriftsinformationen des PDF-Dokuments übernommen.

### 5.2.3 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**: Bei dieser Auswahl wird die Signatur entsprechend der Auswahl im Feld „Standardsignaturformat wählen (CAdES)“ erstellt.
- **XML-Signatur erstellen**: Die Signatur der XML-Datei wird in einer eigenen Datei hinterlegt (XAdES detached). Die Signatur wird in einer zweiten Datei mit der zusätzlichen Dateiendung `sig` abgelegt.

### 5.2.4 Zeitstempel

Wenn Ihr Diensteanbieter einen Zeitstempeldienst konfiguriert hat, können Sie hier die Checkbox „Zeitstempel anbringen“ auswählen.

- **Zeitstempel anbringen**: Sie haben die Möglichkeit, das Anbringen von externen Zeitstempeln zu aktivieren. Lesen Sie hierzu Kapitel 8.1.

## 5.3 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 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. 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.

### Signieren mit dem Signaturdienst

Wenn der Signaturdienst konfiguriert wurde, kann hier auch die Auswahl „DATA Deneb Signaturdienst“ ausgewählt werden. In diesem Fall wird der Auswahl-Button in der nachfolgenden Abbildung zusätzlich angezeigt. Das Signieren mit dem Signaturdienst ist im Kapitel 8.2 erklärt.


Abbildung 10: Auswahl-Button zum Signieren mit dem Signaturdienst

| | |
|---|---|
| | **Hinweis**: Wenn Sie auf den Button DATA Deneb Signaturdienst klicken, wird der Login-Dialog für den Authentisierungsdienst angezeigt. Geben Sie hier die Login-Daten ein. Diese Daten haben Sie üblicherweise von Ihrem Diensteanbieter erhalten. |

Wenn Sie „DATA Deneb Signaturdienst“ ausgewählt haben, wird der Login-Dialog für den Authentisierungsdienst angezeigt. Diese Login-Daten müssen nur einmal eingegeben werden. DATA Boreum speichert diese Daten im temporären Speicher (Cache). Nur wenn Sie DATA Boreum beenden und erneut aufrufen, müssen Sie diese Login-Daten erneut eingeben.

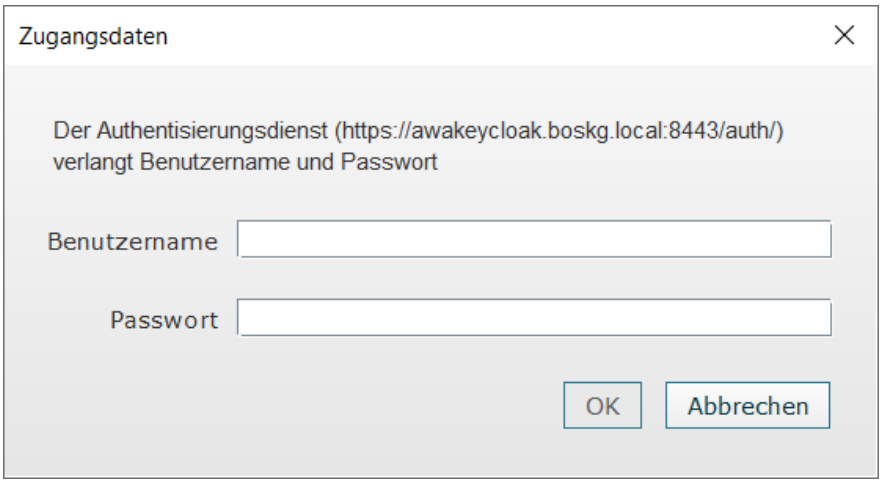


Abbildung 11: Login-Dialog für den Authentisierungsdienst

### BNotK Fernsignaturdienst

Um den Fernsignaturdienst der BNotK benutzen können, benötigen Sie eine Authentisierungskarte, die dazugehörige PIN und ein Chipkartenleser. Stecken Sie die Authentisierungskarte der BNotK in den Chipkartenleser und geben Sie die PIN ein. Es wird der Name des Schlüssels angezeigt, den Sie für Fernsignaturen benutzen können.

### Merkmale für die Schlüsselauswahl des BNotK Fernsignaturdienstes

- **Signaturniveau**: Signaturen mit dem BNotK Fernsignaturdienst sind qualifizierte elektronische Signaturen.
- **Beschränkungen**: Sie können eine Datei oder einen Stapel von Dateien zum Signieren dem BNotK Fernsignaturdienst übergeben. Ein Stapel darf nicht mehr als **100** Dateien umfassen.
- **Dauer der Authentisierung**: Die Authentisierung durch die Eingabe der PIN erzeugt eine Session die bis zu einer Stunde gültig ist. Es können also mehrere Signaturvorgänge nacheinander durchgeführt werden. Nach Ablauf der Gültigkeit muss der BNotK Fernsignaturdienst erneut als Schlüssel ausgewählt und die PIN eingegeben werden.

| | |
|---|---|
|  | **Hinweis**: Wenn Sie den BNotK Fernsignaturdienstes nutzen möchten, muss diese Option durch Ihren Diensteanbieter vorkonfiguriert sein. |

### Schlüssel wählen

Wenn Sie einen Speicherort ausgewählt haben (Datei, Kartenleser, Signaturdienst), werden im darunterliegenden Dialogabschnitt die verfügbaren Schlüssel über die korrespondierenden Zertifikate 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 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.
  - Über den Button  können Sie direkt eine Online-Prüfung des Zertifikats durchführen. Das Prüfprotokoll wird in einem separaten Fenster angezeigt.

### 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. |

## 5.4 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.

## 5.5 Signieren

In der Liste werden alle Dateien aufgeführt, die Sie bei der Dateiauswahl ausgewählt haben, siehe Kapitel 5.1.

### 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 `docx`. **Hinweis**: Lesen dazu bitte auch unbedingt den folgenden Abschnitt "Mindestanzahl einzusehender Dateien".

  Wenn Sie bereits signierte Dateien ausgewählt haben, ist das Lupe-Symbol, mit dem das zur Dateiendung passende Anzeigeprogramm zusammen mit der Datei aufgerufen werden kann, hier eingeschränkt nutzbar. PAdES signierte PDF-Dateien können angezeigt werden. Alle anderen signierte Dateien haben die Endung p7s. CAdES enveloping signierte Dateien mit genau einer Signatur können ebenfalls mit dem zur Dateiendung der Originaldatei passenden Anzeigeprogramm geöffnet werden. Alle anderen CAdES enveloping signierten Dateien lassen sich nicht mit dem zur Originaldatei passenden Anzeigeprogramm öffnen.

- **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.

### 5.5.1 Signieren-Button

Mit dem Signieren-Button am unteren Rand des Dialogfensters lösen Sie den Signaturvorgang aus und es werden nacheinander alle Dateien signiert, die in der Liste aufgeführt sind.

#### Unterer Dialogabschnitt der Funktion Signieren

Im unteren Dialogabschnitt der Funktion Signieren werden unterhalb der Dateiliste und der Auswahl des Nachfolgeprogramms die Einstellungen zusammengefasst, die Sie für diesen Signiervorgang getroffen haben. Sie können die Einstellungen vor dem Signieren erneut ändern, indem Sie zur Dialogseite "Optionen" zurückkehren.

#### 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 in der WebEdition verwenden oder wenn Sie eine andere Signaturkarte verwenden, als die, die zuvor in der WebEdition 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 WebEdition aus Sicherheitsgründen nur verschlüsselt erfolgen darf. Es werden Verschlüsselungszertifikate zwischen dem Kartenleser und der WebEdition 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.

### Login-Dialog bei Anforderung von Zeitstempeln

Wenn Sie auf der Dialogseite „Optionen“ unten auf der Seite die Checkbox „Zeitstempel anbringen ausgewählt haben, siehe Kapitel 5.2.4, wird Ihnen nach dem Klicken auf den „Signieren“-Button der Login-Dialog für den Authentisierungsdienst angezeigt.

| | |
|---|---|
|  | **Hinweis**: Die Login-Daten haben Sie üblicherweise von Ihrem Diensteanbieter erhalten.<br>**Ausnahme**: Wenn Sie zusätzlich zur Option „Zeitstempel anzubringen“ auch das Signieren mit dem DATA Deneb Signaturdienst ausgewählt haben, wird der Login-Dialog nicht angezeigt, weil Sie diese Daten bereits bei der Schlüsselauswahl eingegeben haben, siehe Kapitel 5.3. Diese Login-Daten müssen nur einmal eingegeben werden. DATA Boreum speichert diese Daten im temporären Speicher (Cache). Nur wenn Sie DATA Boreum beenden und erneut aufrufen, müssen Sie diese Login-Daten erneut eingeben. |

Es wird der Login-Dialog für den Authentisierungsdienst angezeigt.

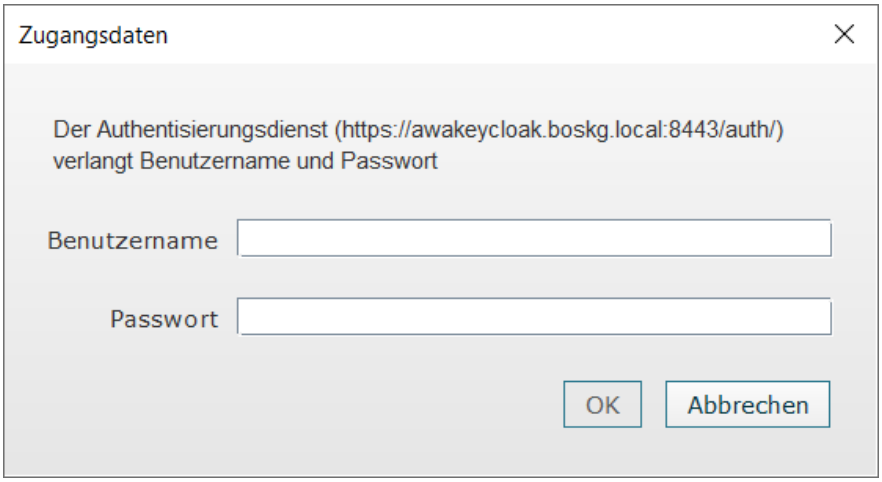


Abbildung 12: Login-Dialog für den Authentisierungsdienst

### 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.

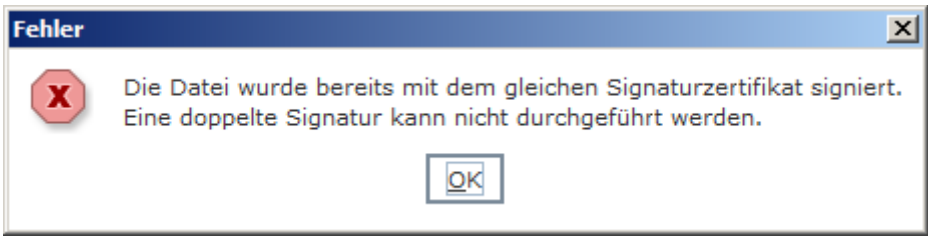


Abbildung 13: Warndialog bei doppelter Signatur

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.

#### 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 vom Dienstanbieter eingestellt. 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 Ihre Administration 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 5.6" Erweiterte PDF-Signatur" beschrieben.

### 5.5.2 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 Validierung 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.

### 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 (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**: Bei dieser Auswahl wird die Signatur entsprechend der Auswahl im Feld „Standardsignaturformat wählen (CAdES)“ erstellt.
- **XML-Signatur erstellen**: Die Signatur der XML-Datei wird in einer eigenen Datei hinterlegt (XAdES detached). Die Signatur wird in einer zweiten Datei mit der zusätzlichen Dateiendung `sig` abgelegt.

### Zeitstempel

Dieses Feld kann die Werte "Ja" und "Nein" haben. Wenn "Ja" angezeigt wird, wird der Signatur ein signierter Zeitstempel 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.

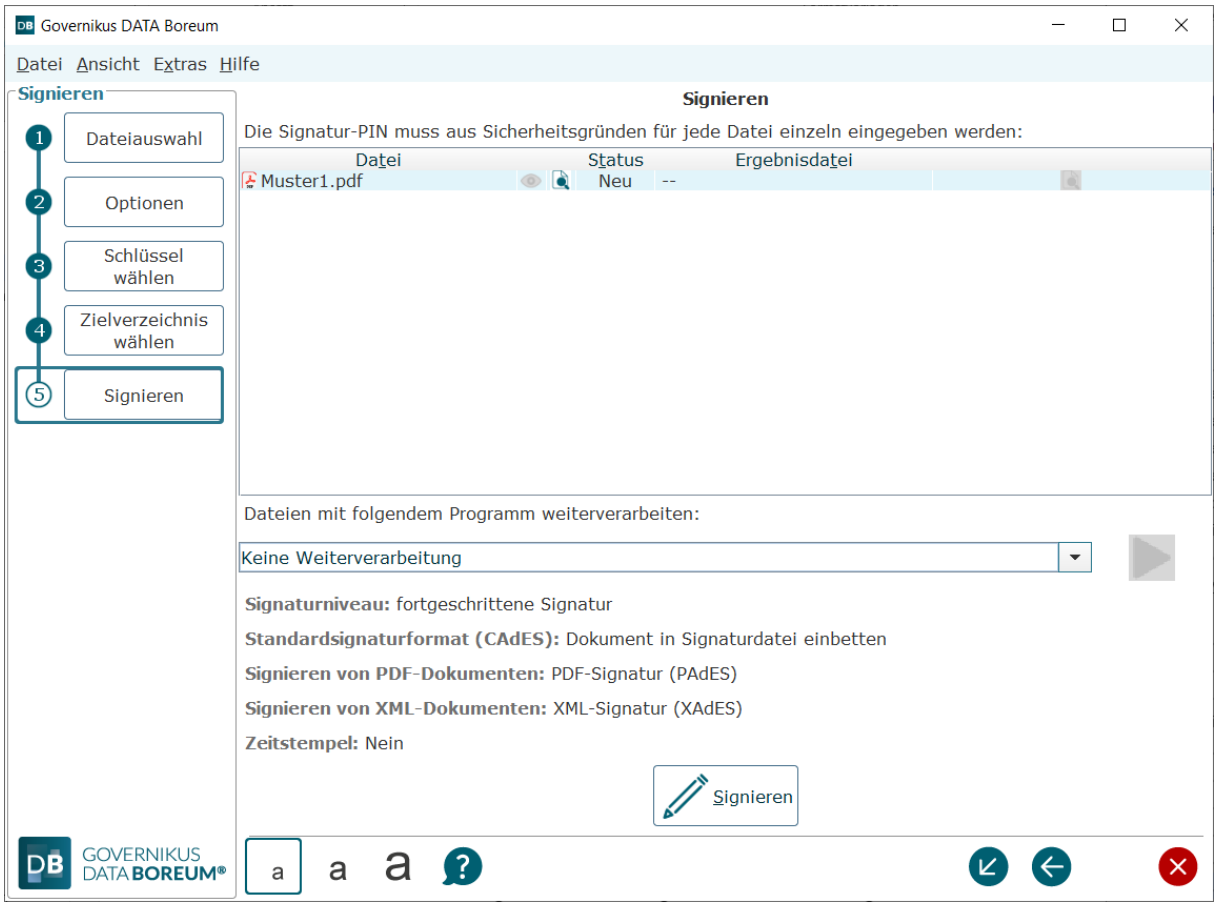


Abbildung 14: Dialogseite Signieren

### 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.

### 5.5.3 Sonderfälle geschützte PDF-Dateien und leere Dateien

#### Sonderfall geschützte PDF-Datei

PDF-Dokumente können gegen Veränderungen geschützt werden und sind damit zum Teil oder vollständig verschlüsselt. In diesem Fall kann keine PAdES-Signatur erstellt werden.

Wenn im Stapel der zu signierenden Dateien eine geschützte PDF-Datei enthalten ist, wird dies von DATA Boreum erkannt. Das Icon am Anfang der Zeile in der Liste der Dokumente zeigt dann einen gelben Kreis mit einem schwarzem Ausrufezeichen .

#### Sonderfall leere Datei

Eine leere Datei wird nicht signiert, da sie keine zu signierenden Inhalte enthält. In diesem Fall wird am Anfang der Zeile in der Liste der Dokumente ein Icon mit einem weißen Kreuz in einem roten Kreis angezeigt .

#### Warnung bei der Verarbeitung geschützter PDF-Dateien oder leerer Dateien

Geschützte PDF-Dateien oder leere Dateien werden nicht signiert. Trifft der Signaturprozess auf  so eine Datei, wird die Verarbeitung gestoppt. Ein Fehlerdialog bietet an, den gesamten Verarbeitungsvorgang zu beenden oder die geschützte PDF-Datei oder leere Datei zu ignorieren und den Prozess mit den nachfolgenden Dateien fortzusetzen.

Die folgende Abbildung zeigt die Dialogseite „Dateiauswahl“ mit einer beispielhafte Dateiliste, in der eine geschützte PDF-Datei und eine leere Datei enthalten sind, die von DATA Boreum korrekt erkannt und markiert werden.

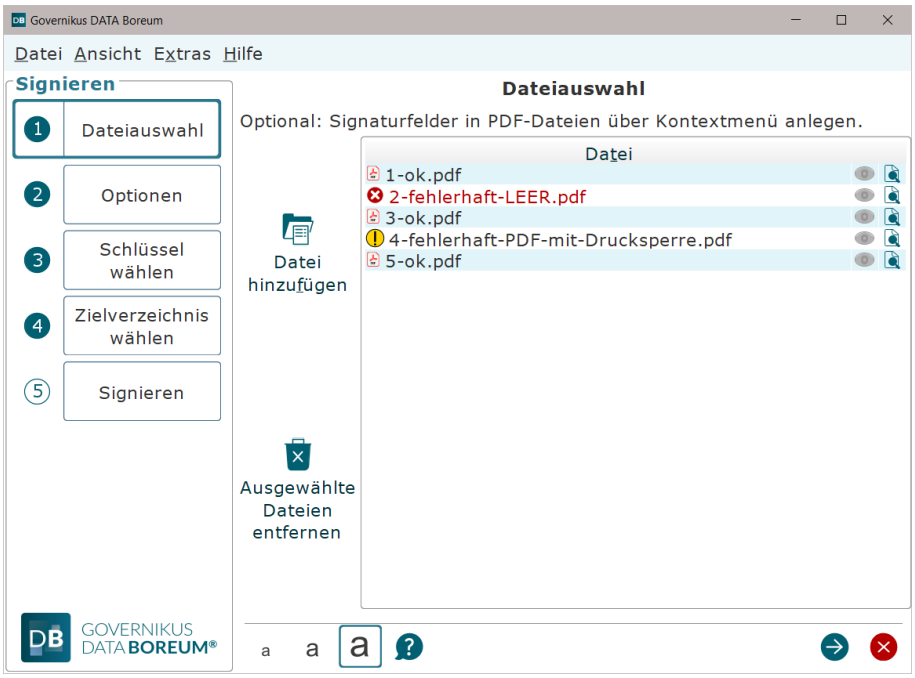


Abbildung 15: Dialogseite „Dateiauswahl“ mit geschützter PDF-Datei und leerer Datei

Die folgende Abbildung zeigt ein Bespiel für einen Hinweisdialog, der angezeigt wird, wenn DATA Boreum bei der Verarbeitung eines Dateistapels auf eine geschützte PDF-Datei stößt. Sie können den Signaturvorgang für diese Datei und alle nachfolgenden fehlerhaften Dateien ignorieren. In diesem Fall werden nachfolgende nicht-fehlerhafte Dokumente signiert. Oder Sie können den Signaturvorgang abbrechen. In diesem Fall werden nachfolgende nicht-fehlerhafte Dateien nicht signiert.

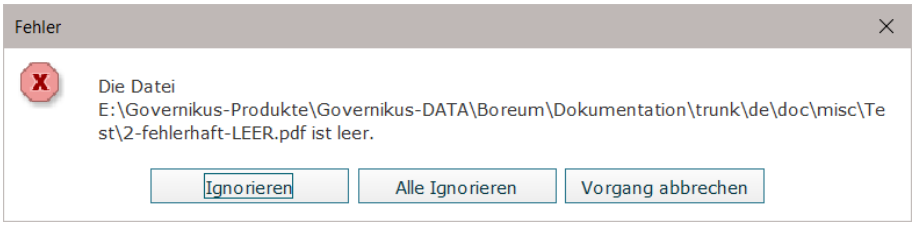


Abbildung 16: Hinweisdialog bei geschützter PDF-Datei

Die folgende Abbildung zeigt die Fehlermeldung, die angezeigt wird, wenn der Signaturvorgang wegen einer leeren Datei angehalten wurde.


Abbildung 17: Hinweisdialog bei leerer Datei

Wenn die Verarbeitung bis zum Ende durchgeführt wurde, wobei geschützte PDF-Dateien und leere Dateien ignoriert wurden, wird am Ende eine weitere Fehlermeldung gezeigt. Dieser Dialog weist daraufhin, dass möglicherweise definierte Folgeprozesse nicht ausgeführt werden. Folgeprozesse werden nicht ausgeführt, weil deren Ausführung zu weiteren Fehlern

führen könnte. In der Liste der Ergebnisdateien wird der Status der Verarbeitung für jede Datei aufgeführt.

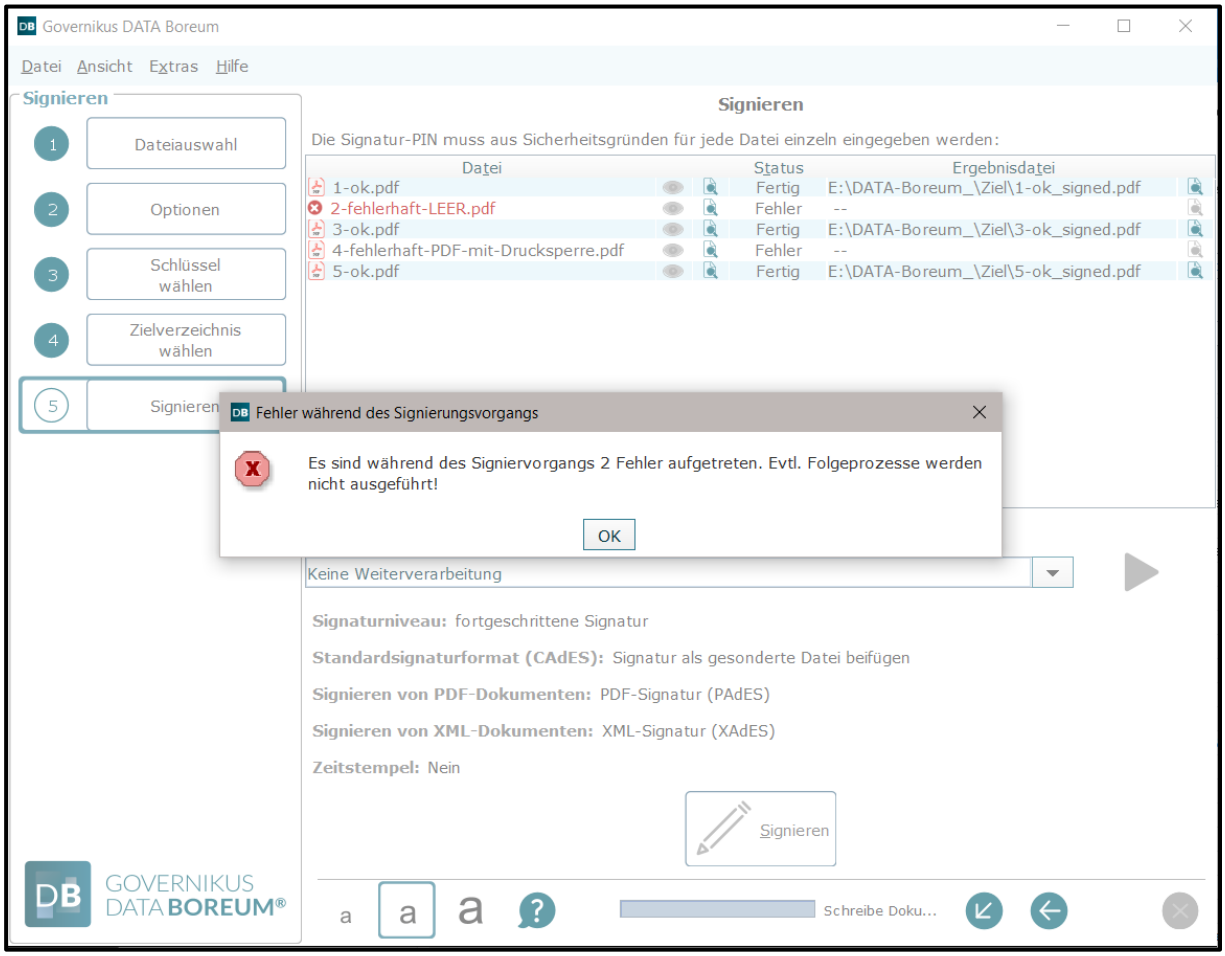


Abbildung 18: Hinweisdialog - keine Ausführung von Folgeprozessen

## 5.6 Erweiterte PDF-Signatur

Wenn Ihre Administration 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.

### 5.6.1 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.

### 5.6.2 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.

# 6 Verschlüsseln mit der WebEdition

Mit dieser Funktion können Sie Dateien verschlüsseln. Eine Erklärung zum Verschlüsseln finden Sie im Kapitel 10.4. 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.

## 6.1 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.

## 6.2 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 10.4.

### 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 10.4 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 10.4 für weitere Informationen zum Verschlüsseln.

## 6.3 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. |

## 6.4 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.

### 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.

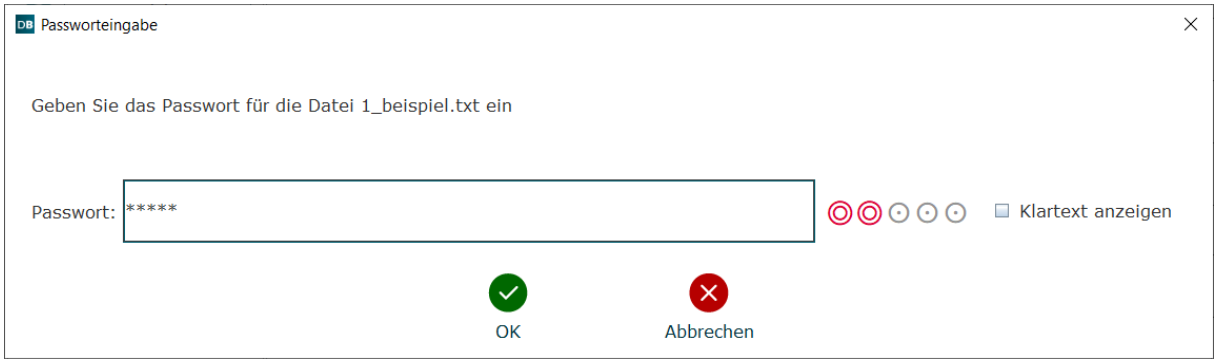


Abbildung 19: Eingabe eines trivialen Passworts - wenige rote Punkte

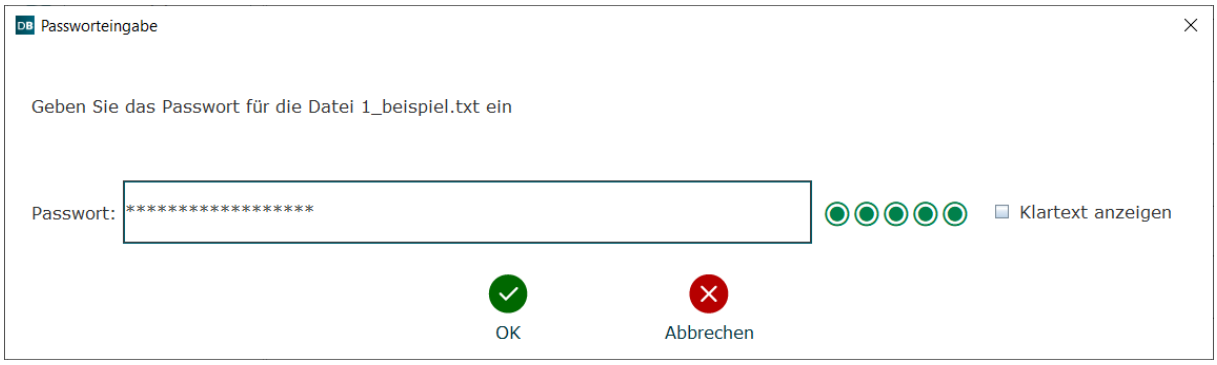


Abbildung 20: Eingabe eines ausreichend sicheren Passworts - alle Punkte grün

### 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.

# 7 Entschlüsseln mit der WebEdition

Mit dieser Funktion können Sie Dateien entschlüsseln. Eine Erklärung zum Entschlüsseln finden Sie im Kapitel 10.4. 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.

## 7.1 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.

## 7.2 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 10.4 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.

## 7.3 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.

## 7.4 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, dass 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.

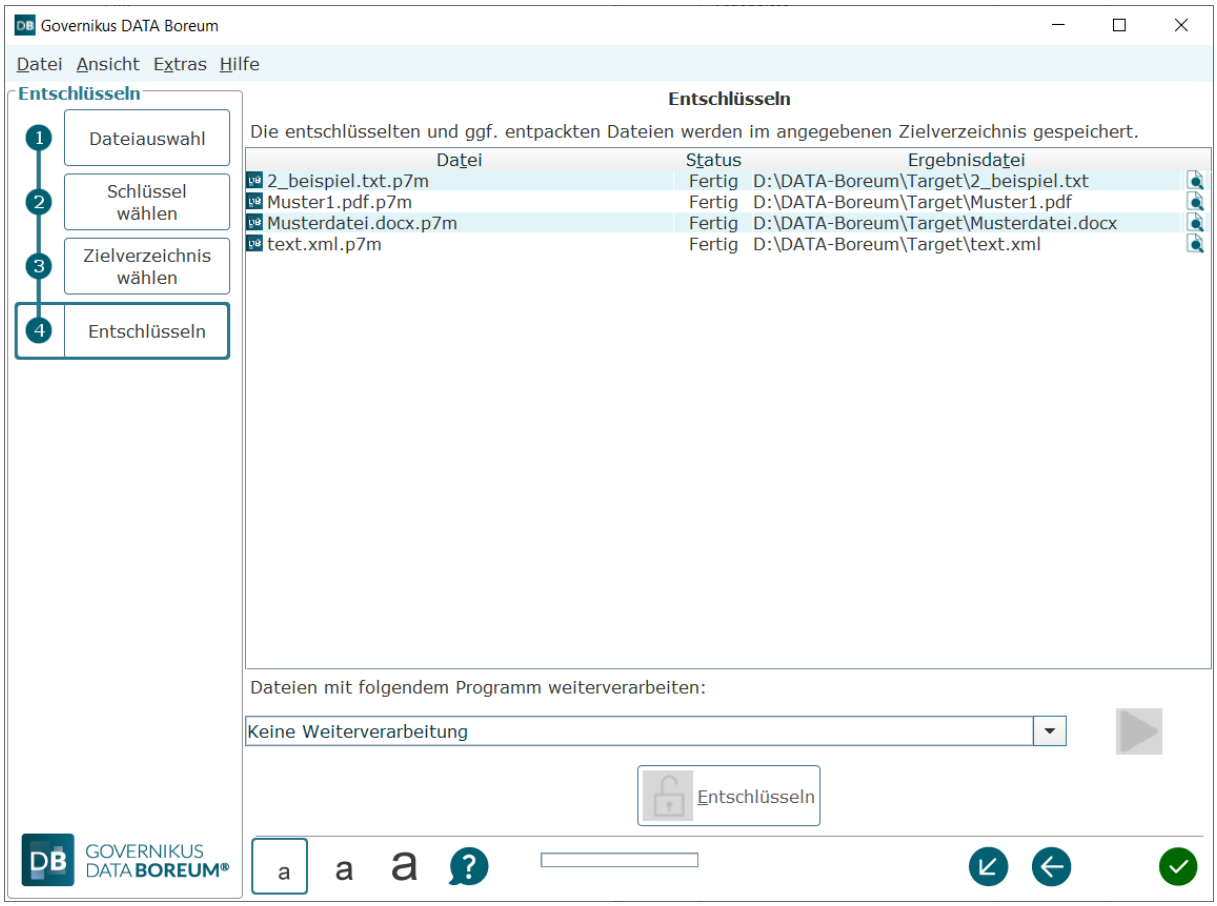


Abbildung 21: Letzte Dialogseite der Funktion Entschlüsseln

# 8 Zusätzliche Funktionen

DATA Boreum bietet folgende, zusätzliche Funktionen:

- **Anbringen externer Zeitstempel**: An eine Signatur oder an ein Siegel kann ein qualifizierter Zeitstempel angebracht werden, siehe nächstes Kapitel.
- **Multisignaturen mit dem Signaturdienst**: Der Signaturdienst ist eine Komponente von DATA Deneb, der sich mit DATA Boreum verbinden lässt, siehe Kapitel 8.2.

## 8.1 Anbringen externer Zeitstempel

DATA Boreum bietet im Rahmen der Signaturerstellung die Option, einer Signatur einen Zeitstempel hinzuzufügen. Nur qualifizierte elektronische Zeitstempel von einem qualifizierten Vertrauensdiensteanbieter sind beweiskräftig und entsprechen den Standards IETF RFC3161 und IETF RFC5816. Gemäß den Standards zur fortgeschrittenen elektronischen Signatur (Advanced electronic Signatures AdES) wird ein Zeitstempel in die Signatur der signierten Datei eingebettet. Es entsteht also keine weitere Datei, die den Zeitstempel enthält, sondern die Signatur selbst wird erweitert.

Nur ein eingebetteter Signaturzeitstempel (Level T) und das nachträgliche Hinzufügen aller Zertifikate und Sperrinformationen (Level LT) sind spezifikationskonform. Wenn die Gültigkeit der Signatur mit Zeitstempel immer wieder verlängert werden soll, muss ein Archivzeitstempel angebracht werden (Level LTA). Der Vertrauensdiensteanbieter für qualifizierte elektronische Zeitstempel bestätigt mit einem qualifizierten Zeitstempel rechtsgültig, dass eine Datei zu dem angegebenen Zeitpunkt vorgelegen hat.

DATA Boreum fordert die Zeitstempel nicht direkt bei den Zeitstempeldienstanbietern an, sondern greift auf einen Zeitstempeldienst zurück. Dieser Zeitstempeldienst ist Bestandteil von DATA Deneb und muss Ihnen von Ihrem Governikus Betreiber bereitgestellt werden. Wenn Ihr Governikus Betreiber einen Vertrag mit einem Zeitstempeldienstanbieter abgeschlossen hat, liefert der Zeitstempeldienst einen qualifizierten Zeitstempel für Ihre elektronische Signatur.

### Konfiguration des Zeitstempeldienstes

Die Konfiguration des Zeitstempeldienstes wird durch Ihren Diensteanbieter vorgenommen und mittels einer Konfiguration beim Starten der Anwendung übergeben. Sie müssen lediglich die Zugangsdaten angeben, die Sie ebenfalls von Ihrem Diensteanbieter erhalten.

## 8.2 Signaturdienst für Multisignaturen

DATA Boreum bietet die Möglichkeit, Signaturen mit dem Signaturdienst zu erstellen. Die Konfiguration des Signaturdienstes wird von Ihrem Diensteanbieter vorgenommen. Über den Signaturdienst können Signaturen nach dem Multisign-Verfahren (umgangssprachlich auch "Massensignaturen" genannt) erstellt werden. Mit so genannten Multisignaturkarten können große Mengen von elektronischen Signaturen angebracht werden. Die Anzahl von Signaturen wird vom Signaturdienst durch Mengen- und Zeitkontingente bestimmt. Sie ist aber nicht - wie bei den "Stapelsignaturkarten" - durch die Signaturkarte begrenzt. Mögliche Einsatzgebiete sind:

- die manuelle Erstellung großer Mengen von Signaturen (kein automatisiertes Verfahren)
- eine räumliche Trennung zwischen dem Arbeitsplatz des Anwendenden und der Signaturinfrastruktur (z. B. Verwendung von Governikus DATA Boreum an einem Scan-

Arbeitsplatz, während der Signaturdienst samt Multisignaturkarte in einem Server-Raum untergebracht sind).

### Einschränkung beim Erstellen von Signaturen mit dem Signaturdienst

Wenn Sie die Erstellung von Signaturen mit dem Signaturdienst ausgewählt haben, beachten Sie bitte, dass pro Signaturauftrag maximal 500 Dateien an den Signaturdienst übergeben werden können. Sie können allerdings beliebig viele Signaturaufträge nacheinander an den Signaturdienst übergeben. Die Begrenzung hat technische Ursachen. DATA Boreum sichert aus Integritätsgründen alle zur Signatur ausgewählten Dateien im Arbeitsspeicher, damit keine unbemerkten Änderungen vorgenommen werden können.

Diese Einschränkung gilt grundsätzlich und nicht nur für das Signieren über den Signaturdienst. Allerdings ist die Möglichkeit, dass mehrere hundert Dateien für das Signieren ausgewählt werden, eher beim Signieren über den Signaturdienst gegeben.

# 9 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 9.2 beschrieben.
- **Security by Design**: Die Governikus KG hat Mechanismen etabliert, um die höchstmögliche Sicherheit ihrer Software zu garantieren. Dies ist in Kapitel 9.3 beschrieben.

## 9.1 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.

### 9.1.1 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.

### 9.1.2 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) der Person, die 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.

### 9.1.3 Technische Anforderungen

Die für den Betrieb der WebEdition unterstützte Hard- und Software ist im Handbuch `Governikus-DATA-Boreum-WE_Systemanforderungen.pdf` 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.

### 9.1.4 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 Ihre WebEdition Administration 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.

## 9.2 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.

### 9.2.1 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.

### 9.2.2 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.

## 9.3 Security by Design

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

### 9.3.1 Überwachung 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-DATA-Boreum-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.

### 9.3.2 Geschützte 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.

### 9.3.3 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.

## 9.4 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 auf dem die Anwendung betrieben wird und dem Download-Server der Governikus KG SSL-verschlüsselt. Die IP-Adresse des Rechners 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 der Person 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 Zertifizierungsdienstanbieter.

#### Konfiguration der WebEdition

Die Konfiguration der WebEdition nimmt die Administration in einem Webserver vor, beispielsweise Tomcat. Ein Anwender hat bei der Benutzung der WebEdition keinen Einfluss auf die Konfiguration, da diese von der Administration vorgegeben ist. Die Konfiguration enthält keine personenbezogenen Daten. Hat der Administration den Aufruf des Dialogs "Einstellungen" für die Person freigeschaltet, kann die Person 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 der Person die die WebEdition betreibt. Folgt die Person den Empfehlungen für den Betrieb, die im Kapitel 8 beschreiben sind, ist ein angemessener Schutz gewährleistet. Die Umsetzung der Empfehlungen liegt in der Verantwortung der Person und ist dem Einfluss der Governikus KG entzogen.

## 9.5 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.

# 10 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.

## 10.1 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.

## 10.2 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.

## 10.3 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.

## 10.4 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. Sie merken beim Betrieb der Anwendung von diesem zweistufigen Verfahren nichts.

## 10.5 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 eingestellt werden kann, ist dieser Signaturzeitpunkt nicht vertrauenswürdig.

## 10.6 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 Validieren von elektronischen Signaturen bestätigt die herausgebende Zertifizierungsstelle die Authentizität desjenigen, der die Signatur angebracht hat.

# 11 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 Anwendungsoberfläche 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.