GOVERNIKUS

GOVERNIKUS
DATA BOREUM®

Anwendungshandbuch
Governikus DATA Boreum

Governikus DATA Boreum, Release 10.6.0

Dokumentenversion: 10.6.0_0

Inhaltsverzeichnis

1 Rechtliche Informationen und weitere Hinweise 5

2 Einführung 6
2.1 Signaturkarten und Siegelkarten 6
2.2 Unterstützte Betriebssysteme 7
2.3 Die Editionen von Governikus DATA Boreum 7
2.4 Überblick über das Anwendungshandbuch 8

3 Installation 9
3.1 DATA Boreum Versionen und Unterschiede 9
3.1.1 Wichtige Unterschiede der MSI und der Portable Versionen 10
3.1.2 SSL-Verbindungen mit DATA Boreum 10
3.2 Installationsdialoge - Windows Installation 11
3.3 Erster Start 14
3.4 Automatische Aktualisierung 14
3.5 Anschließen von Chipkartenleser 16
3.6 Der Lizenzschlüssel 16

4 Schnelleinstieg 18
4.1 Schnelleinstieg Signieren 18
4.2 Schnelleinstieg Validieren 18
4.3 Schnelleinstieg Verschlüsseln 19
4.4 Schnelleinstieg Entschlüsseln 19

5 Einstellungen 20
5.1 Registerkarte Allgemein 20
5.2 Registerkarte Anwendungen 21
5.3 Registerkarte Signieren 24
5.4 Registerkarte Governikus 26
5.5 Registerkarte BNotK 27
5.6 Registerkarte PDF 28
5.6.1 Vorlagen verwalten 29
5.6.2 Visualisierung 31
5.6.3 Signaturfeld platzieren 31
5.6.4 Schrift 33
5.6.5 Grafik 33
5.7 Registerkarte Validierung 34
5.8 Registerkarte Verschlüsseln 36
5.9 Registerkarte Entschlüsseln 37
5.10 Registerkarte Netzwerk 37
5.11 Einstellungen exportieren 39

6 Hauptfunktionen von Governikus DATA Boreum 41
6.1 Menüleiste von Governikus DATA Boreum 41
6.2 Tastaturbefehle 43
6.3 Gemeinsame Merkmale der Dialogseiten 44
6.3.1 Navigation durch die Dialogseiten 45
6.3.2 Dateiauswahl 46
6.3.3 Zielverzeichnis wählen 48
6.4 Signieren 49
6.4.1 Dateiauswahl 49
6.4.2 Sonderfall PDF-Datei 50

6.4.3 Optionen für die Funktion Signieren 53
6.4.4 Schlüssel wählen 55
6.4.5 Zielverzeichnis wählen 63
6.4.6 Signieren 63
6.4.7 Sonderfälle Stapelsignaturkarte und Multisignaturkarte 67
6.5 Validieren 68
6.5.1 Signaturformate 69
6.5.2 Dateiauswahl 70
6.5.3 Optionen für die Funktion Validieren 70
6.5.4 Validieren 71
6.5.5 Das Prüfprotokoll 74
6.6 Verschlüsseln 75
6.6.1 Dateiauswahl 75
6.6.2 Schlüssel wählen 76
6.6.3 Zielverzeichnis wählen 78
6.6.4 Verschlüsseln 78
6.7 Entschlüsseln 81
6.7.1 Dateiauswahl 82
6.7.2 Schlüssel wählen 82
6.7.3 Zielverzeichnis wählen 83
6.7.4 Entschlüsseln 84

7 Zusätzliche Funktionen 87
7.1 Anbringen externer Zeitstempel 87
7.2 Governikus DATA Boreum als Hintergrundprozess 87

8 Besonderheiten der Integration Edition 90
8.1 Konfiguration 90
8.2 Menüleiste der Integration Edition 91
8.3 Optionen über das Tray-Icon aufrufen 92
8.4 Die Funktionen der Integration Edition 92

9 Erläuterungen 94
9.1 Authentifizierung und Authentisierung 94
9.2 Entschlüsselung 94
9.3 Signatur 94
9.4 Signaturalgorithmus 96
9.5 Signaturformate 96
9.6 Signaturkarte 97
9.7 Validieren 97
9.8 Verschlüsselung 98
9.9 Zeitstempel 99
9.10 Zertifizierungsstelle 99

10 Sicherheit und Datenschutz 100
10.1 Empfehlungen für den Betrieb 100
10.1.1 Empfohlene Anforderungen an die Einsatzumgebung 100
10.1.2 Empfehlungen für den sicheren Betrieb 101
10.1.3 Technische Anforderungen 101
10.1.4 Anforderungen an die Konfiguration 101
10.2 Privacy by Design 102
10.2.1 Privacy by Design - Produktentwicklung 102
10.2.2 Privacy by Default - Produktkonfiguration 102
10.3 Security by Design 102
10.3.1 Überwachung von Drittanbieter-Produkten 102

10.3.2 Geschützte Produktionsumgebung 103
10.3.3 Bewertung von Gefährdungen 103
10.4 DSGVO und Governikus DATA Boreum 103
10.5 Gesetzliche Grundlagen 105

11 Erste Hilfe 106

12 Ablage von Daten bei Nutzung des Installers 109
12.1.1 Installation der Anwendung 109
12.1.2 Ablage von log-Informationen 109

13 Barrierefreiheit 110
13.1 Java Access Bridge aktivieren 110
13.2 DATA Boreum und die Umsetzung der Barrierefreiheit 111
13.3 BITV-Test - Liste der Prüfschritte im Testverfahren 113

14 Abbildungsverzeichnis 126

1 Rechtliche Informationen und weitere Hinweise

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

2 Einführung

	**Erklärung**: Governikus DATA Boreum implementiert die europäischen Normen und Standards zur Anbringung und Validierung von elektronischen Signaturen, die beanspruchen, den rechtlichen Anforderungen aus der eIDAS-VO zu genügen.

Governikus DATA Boreum bietet alle Funktionalitäten, die für die Sicherstellung und Prüfung der Integrität und Authentizität von Dateien sowie der Geheimhaltung von Dateiinhalten notwendig sind. Sie können mit Governikus DATA Boreum Dateien signieren, um deren Integrität und Authentizität sicherzustellen. Sie können signierte Dateien validieren, um die Integrität und Authentizität zu überprüfen.

Sie können Dateien verschlüsseln, um den Inhalt geheim zu halten und Sie können Dateien entschlüsseln (wenn Sie über den notwendigen Schlüssel verfügen), um den Inhalt wieder in seine ursprüngliche Form zu bringen.

Sie können diese Verfahren auch kombinieren. Da der Inhalt von Dateien, die "nur" signiert wurden, weiterhin lesbar ist, können Sie die Datei zuerst verschlüsseln und danach die verschlüsselte Datei signieren.

Sollten in Ihren Arbeitsabläufen mit Governikus DATA Boreum bestimmte Einstellungen immer die gleichen sein, können Sie diese entsprechend kennzeichnen. Sie werden dann bei der Arbeit mit Governikus DATA Boreum nicht mehr nach diesen Arbeitsschritten gefragt und die dazugehörigen Dialoge werden übersprungen, wodurch Sie die Arbeit mit Governikus DATA Boreum beschleunigen können.

	**Hinweis**: Governikus DATA Boreum ermöglicht die Erstellung und Prüfung von "qualifizierten elektronischen Signaturen und Siegeln" gemäß eIDAS-Verordnung und ETSI-Spezifikation. Hieraus ergeben sich auch Anforderung an Ihren Arbeitsplatz. Lesen Sie diesbezüglich unbedingt das Kapitel 10.1 "Empfehlungen für den Betrieb". Wenn Sie mit mit elektronischen Signaturen nicht vertraut sind, sollten Sie die Erläuterungen zur elektronischen Signatur, Signaturkarten und Validierung in Kapitel 9 "Erläuterungen" lesen.

Die fachlichen Hintergründe zu den Funktionen von Governikus DATA Boreum werden im Kapitel 9 "Erläuterungen" erklärt. In den Kapiteln zu den Funktionen von Governikus DATA Boreum werden diese Erklärungen daher weggelassen und es werden direkt die Dialoge und die Benutzerführung erklärt.

2.1 Signaturkarten und Siegelkarten

Mit Governikus DATA Boreum kann mit einem geeigneten Chipkartenleser und einer Signaturkarte eine qualifizierte elektronische Signatur für eine Datei erstellt werden. Ebenso kann mit Governikus DATA Boreum mit einem geeigneten 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, siehe eIDAS-Verordnung, Abschnitt 4, Artikel 25, Ziffer 2.
- **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, siehe auch eIDAS Verordnung Abschnitt 5, Artikel 35.

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.

2.2 Unterstützte Betriebssysteme

Governikus DATA Boreum kann auf diesen Betriebssystemen betrieben werden:

- Windows,
- Linux und
- macOS

Für jedes Betriebssystem gibt es eine eigene Installationsdatei. Welche Versionen der jeweiligen Betriebssysteme unterstützt werden, entnehmen Sie bitte dem Handbuch `Governikus-DATA-Boreum_Systemanforderungen.pdf`. Für die Betriebssysteme Windows und Linux gibt es keine funktionalen Unterschiede.

Hinweis: Für das Betriebssystem macOS wird jeweils gesondert in eigenen Absätzen daraufhin hingewiesen, wenn Abweichungen bestehen. Diese Absätze werden mit dem Schlüsselwort macOS eingeleitet.

2.3 Die Editionen von Governikus DATA Boreum

Governikus DATA Boreum

Diese Edition bietet die Funktionen Signieren, Validieren, Verschlüsseln und Entschlüsseln. Es ist zudem möglich, den DATA Deneb Signaturdienst der Governikus Suite für die Erstellung von Multisignaturen anzusprechen. Des Weiteren können Zeitstempel angefordert werden. Diese Funktionen werden im Kapitel 7 beschrieben.

Governikus DATA Boreum Integration Edition

Die Governikus DATA Boreum Integration Edition wird durch andere Anwendungen aufgerufen und ermöglicht so die einfache Integration von Signatur- und Validierungsfunktionen sowie Ver- und Entschlüsselungs-funktionen in Fachanwendungen. Der Aufruf kann über einen Webservice (SOAP), die Java-API oder Kommandozeile erfolgen. Es gibt allerdings einige Unterschiede, die im Kapitel 8 erklärt werden.

2.4 Überblick über das Anwendungshandbuch

Das vorliegende Handbuch unterteilt sich in folgende Hauptkapitel:

- **Einführung**: Dieses vorliegende Kapitel.
- **Installation**: Erklärt die Schritte beim Installieren von Governikus DATA Boreum auf Ihrem Rechner und verweist auf die Hard- und Softwarevoraussetzungen für die Benutzung von Governikus DATA Boreum. Dies ist Kapitel 3.
- **Schnelleinstieg**: Erklärt kurz und knapp die grundlegenden Schritte für alle Funktionen. In jedem Schritt wird auf das dazugehörige Kapitel mit ausführlichen Erläuterungen verwiesen. Dies ist Kapitel 3.6.
- **Einstellungen**: Erklärt die zentrale Konfiguration von Governikus DATA Boreum. Diese Einstellungen müssen Sie nur einmal vornehmen. Sie können den Dialog aber jederzeit erneut aufrufen, wenn Sie Einstellungen ändern wollen. Dies ist Kapitel 5.
- **Hauptfunktionen**: Leitet die Beschreibungen der folgenden vier Hauptfunktionen ein. Es erklärt zuerst die Dialogteile, die bei allen Funktionen gleich sind. Dies ist Kapitel 6.
- **Signieren**: Erklärt das Vorgehen für das elektronische Signieren einer oder mehrerer Dateien. Dies ist Kapitel 6.4.
- **Validieren**: Erklärt das Vorgehen für den Nachweis von Integrität und Authentizität einer elektronisch signierten Datei. Dies ist Kapitel 6.5.
- **Verschlüsseln**: Erklärt das Vorgehen für das Umwandeln einer Datei in eine geheime Repräsentation. Dies ist Kapitel 6.6.
- **Entschlüsseln**: Erklärt das Vorgehen für das Rückwandeln einer Datei von einer geheimen in die Ausgangsrepräsentation. Dies ist Kapitel 6.7.
- **Weitere Funktionalitäten**: Erklärt die Funktionen Massensignaturen, Zeitstempel und Governikus DATA Boreum als Hintergrundprozess. Dies ist Kapitel 7 beschrieben.
- **Integration Edition**: Beschreibt die Besonderheiten der Integration Edition. Dies ist Kapitel 8.
- **Erläuterungen**: Erklärt Begriffe und Hintergründe, die im Kontext von Governikus DATA Boreum wichtig sind. Dies ist Kapitel 9.
- **Weitere Anforderungen**: Beschreibt die Anforderungen an den Betrieb von Governikus DATA Boreum in Übereinstimmung mit der eIDAS-Verordnung. Dies ist Kapitel 10.1.
- **Erste Hilfe**: Bietet Hinweise und Lösungen bei möglicherweise auftretenden Problemen bei der Benutzung von Governikus DATA Boreum. Dies ist Kapitel 11.
- **Barrierefreiheit**: Die Benutzeroberfläche von DATA Boreum ist weitestgehend barrierefrei umgesetzt. Kapitel 12 beschreibt die Umsetzung:

3 Installation

Voraussetzungen

Bitte lesen Sie das Dokument "Governikus DATA Boreum Systemanforderungen" vor der Installation. Hier werden die Voraussetzungen für die Installation erklärt. Darüber hinaus stehen Ihnen Dokumente zur Verfügung, die Sie darüber informieren, welche Signaturkarten und Chipkartenleser unterstützt werden. Die Handbücher von Governikus DATA Boreum finden Sie im Portal der Governikus KG.

Prüfung der Softwareintegrität

Die Funktionen Signieren und Validieren sind sicherheitskritische Funktionen. Prüfen Sie vor der Installation auf jeden Fall die Integrität der Software, um die Installation von manipulierter Software zu vermeiden.

Die Prüfung der Integrität erfolgt über einen Hashwert-Vergleich. Die Governikus KG bietet auf der Portalseite der Governikus KG im jeweiligen Produktbereich den Hashwert (Algorithmus SHA-256) an.

Zur Prüfung ist es erforderlich, dass Sie zum vorliegenden Installationsprogramm von Governikus DATA Boreum ebenfalls einen Hashwert berechnen und prüfen, ob dieser mit dem durch die Governikus KG veröffentlichten Hashwert zu dieser Version von Governikus DATA Boreum übereinstimmt.

Bitte prüfen Sie auch, ob die vorliegende Dokumentation zu der Software-Version gehört. In jedem Dokument ist auf dem Deckblatt die Release-Nummer der Software vermerkt. Vergleichen Sie diese Nummer mit der Release-Nummer aus dem Namen der Installationsdatei oder nach der Installation über das Informationsfenster "Über Governikus DATA Boreum", siehe Kapitel 6.1.

3.1 DATA Boreum Versionen und Unterschiede

Berechtigungen

Die Installation mit dem MSI-Installer, siehe nächster Absatz, muss mit Administrator-Berechtigungen durchgeführt werden. Es muss die Berechtigung bestehen, die Anwendung im gewählten Installationsverzeichnis zu installieren sowie (unter MS Windows) systemübergreifende Registry-Einträge zu erstellen. Die Anwendung selber kann mit normalen Benutzerberechtigungen gestartet werden.

Installationsschritte für Windows und Linux

- **Windows**: Für das Betriebssystem Windows wird Governikus DATA Boreum als ausführbare Datei geliefert. Wenn Sie diese aufrufen, werden Sie schrittweise durch die Dialogseiten der Installation geführt, auf denen Sie einige Einstellungen bestimmen können. Nach dem Anfangsdialog können Sie über den Zurück-Button immer wieder zur vorherigen Dialogseite zurückkehren, falls Sie Korrekturen vornehmen wollen. Der Verlauf der Installation ist der gleiche für alle Editionen von Governikus DATA Boreum.
- **Linux**: Für das Betriebssystem Linux wird Governikus DATA Boreum als Archivdatei ausgeliefert. Diese muss im gewünschten Verzeichnis entpackt werden. Beim ersten Aufruf von Governikus DATA Boreum beachten Sie bitte die Schritte, die im Kapitel 3.3 erklärt sind.

- **macOS**: Für macOS wird Governikus DATA Boreum als Archivdatei ausgeliefert. Sie enthält die jeweiligen Installationsdateien als `app`-Datei, die in das Applications-Verzeichnis gezogen werden kann und dort mit einem Doppelklick ausgeführt wird.

Mit und ohne automatische Softwareaktualisierung - Offline- und Online-Version

Für die Installation von Governikus DATA Boreum werden für das Windows-Betriebssystem unterschiedliche Installationsdateien angeboten:

Windows

- `DataBoreum_<Versionsnummer>.msi`
- `GovernikusDataBoreumPortable_<Versionsnummer>_Offline.zip`

3.1.1 Wichtige Unterschiede der MSI und der Portable Versionen

Windows-Installationsdatei (MSI) - JDK enthalten

Die Windows-Installationsdatei (MSI) installiert Governikus DATA Boreum mit der automatischen Aktualisierungsfunktion, das heißt, bei jedem Start von DATA Boreum wird auf eine aktuelle Version geprüft. Für die Aktualisierungsabfrage muss der Port 443 freigeschaltet sein. Die automatische Aktualisierung ist im Kapitel 3.4 beschrieben. Zudem wird für DATA Boreum eine eigene Java-Laufzeitumgebung (JDK) installiert, die über die MSI-Datei ausgeliefert wird. Damit ist DATA Boreum unabhängig von möglicherweise vorhandenen weiteren Java-Versionen. Sie können daher diese Java-Versionen auch aktualisieren, ohne das DATA Boreum davon beeinflusst wird. Auch Pfadangaben für diese anderen JDKs oder möglicherweise gesetzte `JAVA_HOME`-Umgebungsvariablen beeinflussen das JDK von DATA Boreum nicht.

Portable-Version - JDK nicht enthalten

Die Governikus DATA Boreum und Governikus DATA Boreum **Integration Edition** und die Versionen für die Betriebssysteme **Linux** und **macOS** sind nur in der Offline Version verfügbar. Offline bedeutet in diesem Kontext, dass DATA Boreum keine Verbindung zum Aktualisierungs-Server der Governikus KG aufbaut, sondern mit den vorhandenen Ressourcen startet. Die Offline oder auch Portable genannte Version, setzt eine Java-Laufzeitumgebung (JDK) voraus. Diese DATA Boreum Version wird mit einer Batch-Datei gestartet. Sie müssen vor dem ersten Start ein JDK installiert haben und dieses JDK muss der Pfadangabe des Betriebssystems hinzugefügt werden, damit DATA Boreum auf das JDK zugreifen kann.

3.1.2 SSL-Verbindungen mit DATA Boreum

Wenn Sie den DATA Deneb Signaturdienst in DATA Boreum konfiguriert haben, siehe Kapitel 5.4, sind die Verbindungen zwischen DATA Boreum und dem Authentisierungsserver und dem DATA Deneb Signaturdienst über SSL abgesichert. Auf den Servern, auf denen der Authentisierungsdienst und der DATA Deneb Signaturdienst betrieben werden, müssen in den SSL-Keystores und Truststores SSL-Zertifikate hinterlegt sein, die von offiziellen Vertrauensdiensteanbietern (certificate authorities) stammen, wie beispielsweise D-Trust oder TeleSec. Sollten Sie SSL-Zertifikate aus einer eigenen PKI oder andere selbstsignierte SSL-Zertifikate nutzen, kann keine SSL-Verbindung aufgebaut werden, da es keine Möglichkeit in DATA Boreum gibt, diese SSL-Zertifikate zu hinterlegen.

Workaround SSL-Zertifikate

Sollten Sie die SSL-Strecken mit eigenen SSL-Zertifikaten gesichert haben, können Sie diese im Truststore der Java-Laufzeitumgebung (JDK) hinterlegen. Dies ist der Ort, an dem DATA Boreum nach vertrauenswürdigen SSL-Zertifikaten sucht.

- **JDK-Truststore**: Den Truststore eines JDKs finden Sie üblicherweise in diesem Pfad:

  `<JDK-Installationsverzeichnis>/lib/security`

- **Truststore-Name**: Der Truststore heißt üblicherweise `cacerts` (ohne weitere Dateiendung).
- **Truststore-Passwort**: Das Passwort für die Datei `cacerts` ist üblicherweise `changeit`
- **SSL-Zertifikate hinzufügen**: Fügen Sie ihre eigenen SSL-Zertifikate des Authentisierungsdienstes und des DATA Deneb Signaturdienstes als „Vertrauenswürdige Zertifikate“ diesem Truststore hinzu.
- **Neustart**: Starten Sie DATA Boreum danach neu.

3.2 Installationsdialoge - Windows Installation

Die folgende Beschreibung zeigt die Installation für das Betriebssystem Windows. Für das Betriebssystem Linux verfahren Sie bitte wie oben im Kapitel 3, Abschnitt Installationsschritte beschrieben.

Dialogseite Willkommen

Der Installationsvorgang beginnt mit der Dialogseite "Willkommen".

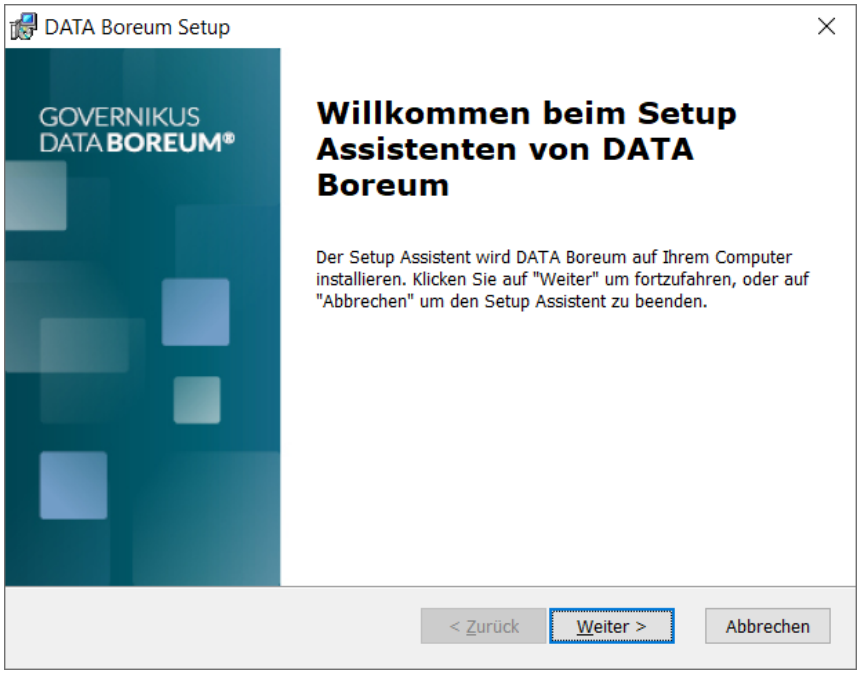

Abbildung 1: Startdialog der Installation

Dialogseite Lizenzvertrag

Lesen Sie in diesem Installationsschritt die Nutzungsbedingungen. Nur wenn Sie den Nutzungsbedingungen zustimmen, können Sie mit der Installation fortfahren.

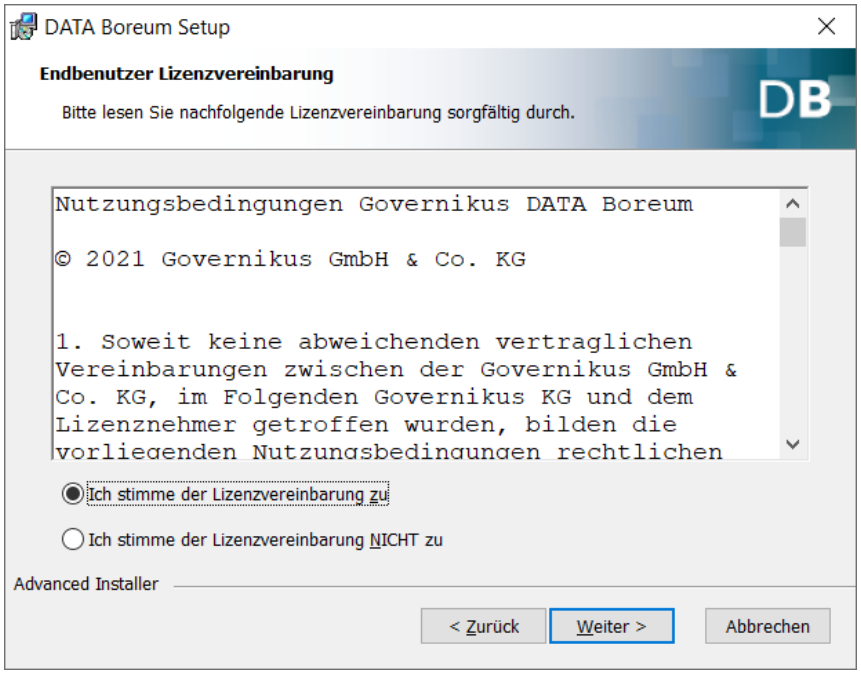

Abbildung 2: Nutzungsbedingungen von Governikus DATA Boreum akzeptieren

Dialogseite Installationsverzeichnis

In diesem Dialog können Sie ein Installationsverzeichnis auswählen oder die Vorauswahl annehmen.

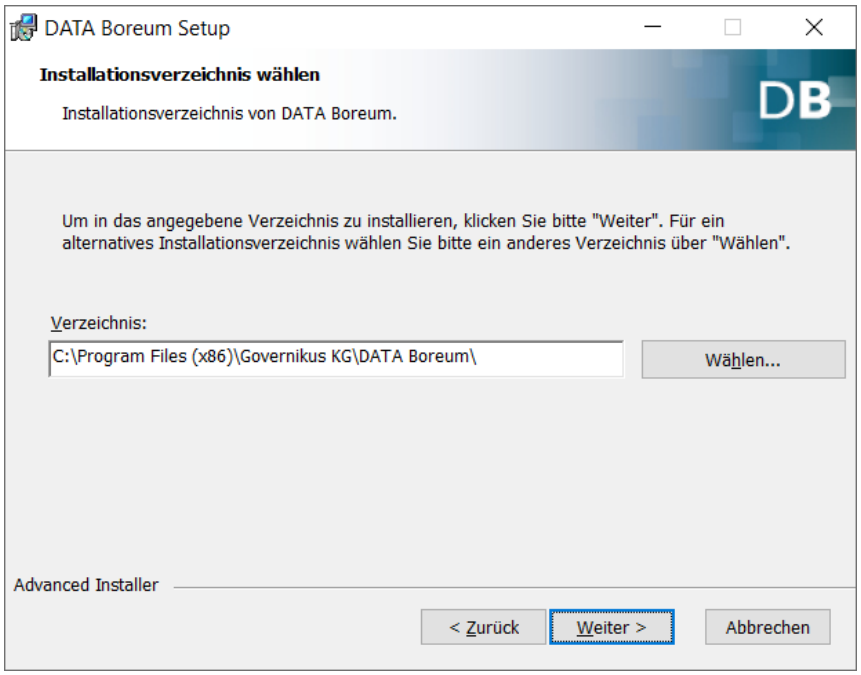

Abbildung 3: Auswahl des Installationsverzeichnisses

Dialogseite Vorbereitung abgeschlossen

Nach diesem Dialog ist die Installationsvorbereitung abgeschlossen. Starten Sie den Installationsvorgang mit dem "Installieren"-Button.

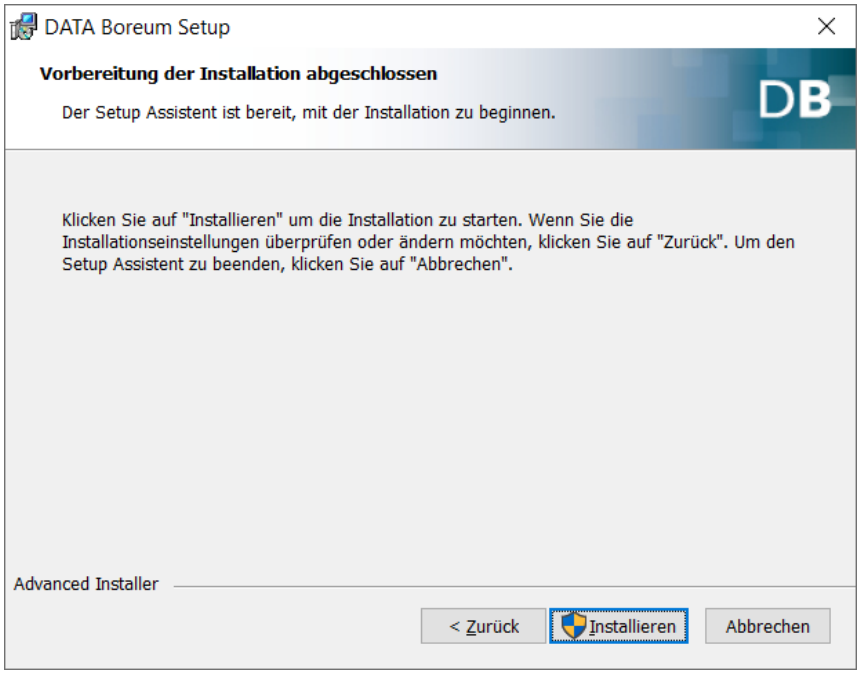

Abbildung 4: Vorbereitung der Installation abgeschlossen

Dialogseite Fertigstellen

Auf dieser Dialogseite beenden Sie den Installationsvorgang. Wenn sie die Checkbox "Governikus DATA Boreum ausführen" auswählen, wird Governikus DATA Boreum anschließend gestartet.

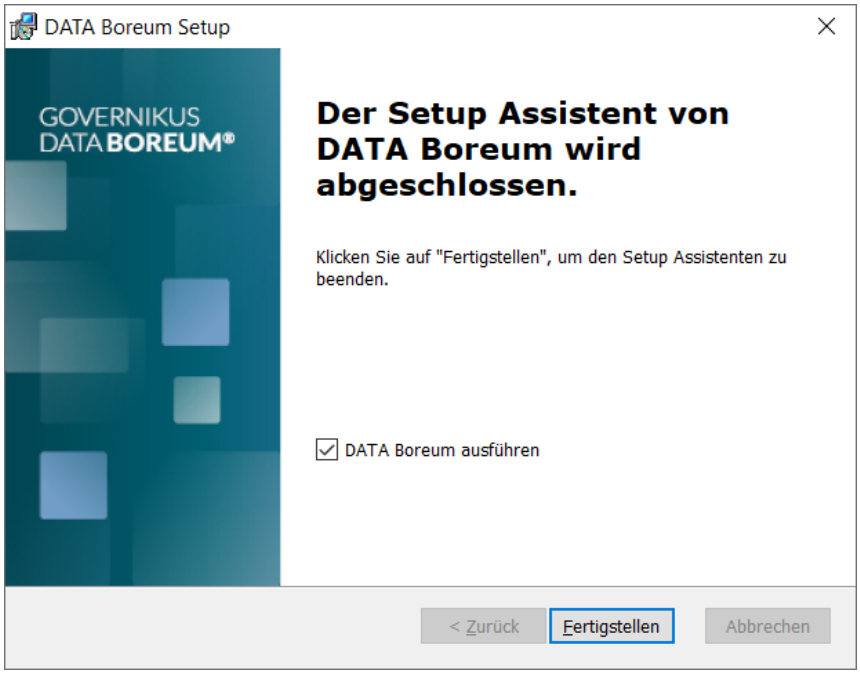

Abbildung 5: Installation fertigstellen

Mit diesem Dialog ist die Installation von Governikus DATA Boreum abgeschlossen. Bitte beachten Sie vor dem ersten Start von Governikus DATA Boreum die anschließenden Kapitel.

3.3 Erster Start

Sie können Governikus DATA Boreum über den Eintrag im Startmenü, über das Kontextmenü einer Datei oder durch Doppelklick auf eine verknüpfte Datei starten. Verknüpfte Dateien sind:

- `p7s`: Datei, die gemäß dem PKCS#7 Standard signiert wurde,
- `p7m`: verschlüsselte oder verschlüsselte und gemäß PKCS#7 Standard signierte Datei,
- `enz`: Datei, die mit einem Passwort verschlüsselt wurde,
- `pkcs7`: Datei, die gemäß dem PKCS#7 Standard signiert wurde.

Hinweis: Für macOS Benutzer steht der Aufruf von Governikus DATA Boreum per Kontextmenü oder per Doppelklick auf eine Datei nicht zur Verfügung.

Governikus DATA Boreum ist mit oder ohne automatische Aktualisierung verfügbar. Haben Sie die Variante ohne automatische Aktualisierung installiert, startet die Anwendung direkt.

3.4 Automatische Aktualisierung

Haben Sie Governikus DATA Boreum mit automatischer Aktualisierung installiert, prüft Governikus DATA Boreum beim jedem Start, ob eine aktuellere Version vorliegt. Dazu verbindet sich Governikus DATA Boreum mit dem Update-Server der Governikus KG. Liegt eine aktuellere Version vor, wird dies durch einen Dialog angezeigt, ansonsten startet Governikus DATA Boreum ohne weitere Meldung.

Wenn eine aktuellere Version vorliegt, können Sie auf dem Dialogfenster über die entsprechenden Buttons entscheiden, wie Sie vorgehen möchten.

- **Ja**: Wenn Sie "Ja" wählen, wird die neue Version installiert.
- **Nicht jetzt**: Wenn Sie "Nicht jetzt" wählen, wird Governikus DATA Boreum gestartet, ohne dass die aktuellere Version installiert wird. Sie werden beim nächsten Start von Governikus DATA Boreum erneut gefragt, ob Sie die neue Version installieren wollen.
- **Nein**: Wenn Sie "Nein" wählen, wird Governikus DATA Boreum gestartet, ohne dass die neue Version installiert wird. Sie werden nicht mehr nach der Installation der neuen Version gefragt. Erst wenn diese neue Version eine Nachfolge-Version hat, wird dieser Dialog wieder angezeigt.

Die folgende Abbildung zeigt den Update-Dialog mit Beispiel-Versionen.

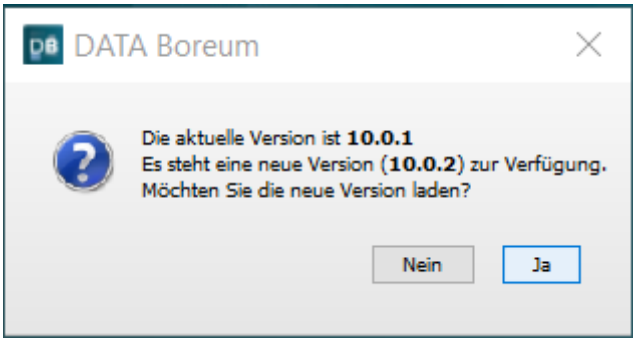

Abbildung 6: Update-Dialog mit Beispiel-Versionen

Fehler: Verbindung zum Update-Server nicht möglich

Wenn keine Verbindung zum Update-Server möglich ist, wird eine Fehlermeldung angezeigt. Auf der Dialogseite der Fehlermeldung haben Sie diese Möglichkeiten:

- **Internetoptionen öffnen**: Dieser Button öffnet die Dialogseite mit den Internetoptionen des Betriebssystems. Ein möglicher Fehler ist, dass Ihr Systemadministrator einen Update-Server im Firmennetz eingerichtet hat. Dieser Update-Server befindet sich dann innerhalb des Firmen-LANs und benötigt keinen Proxy-Server. In diesem Fall fragen Sie Ihren Systemadministrator nach der IP-Adresse des Update-Servers. Wählen Sie dann auf der Dialogseite "Internetoptionen" die Registerkarte "Verbindungen" und klicken Sie unten auf den Button "LAN-Einstellungen". Es wird der der Dialog "Einstellungen für lokale Netzwerke" angezeigt. Über den Button "Erweitert" gelangen Sie in den Dialog "Proxyeinstellungen". Geben Sie die IP-Adresse des Update-Servers im Feld "Ausnahmen" ein. Verwenden Sie das Semikolon, um diesen neuen Eintrag von bereits existierenden Einträgen zu trennen. Geben Sie keine Leerzeichen ein. Bestätigen Sie danach alle offenen Dialogseiten mit dem "OK"-Button.
- **Beenden**: Über diesen Button beenden Sie den Aufruf. Governikus DATA Boreum wird nicht gestartet.
- **Anwendung starten**: Über diesen Button wird Governikus DATA Boreum ohne Verbindung zum Update-Server gestartet. Sie können ganz normal mit Governikus DATA Boreum arbeiten.

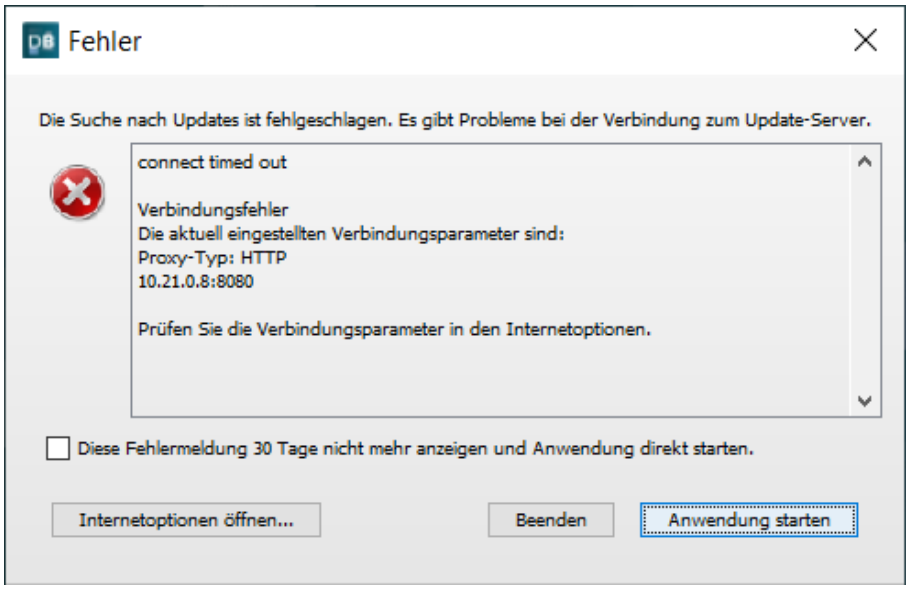

Abbildung 7: Verbindung zum Update-Server nicht möglich

3.5 Anschließen von Chipkartenleser

Chipkartenleser, die über einen USB-Anschluss mit dem Computer verbunden sind, erfordern üblicherweise keine weiteren Installationsschritte durch die Anwender. Beachten Sie hierzu auch die Dokumentation Ihres Chipkartenlesers. Wenn Sie Chipkartenleser unter Linux betreiben, muss zusätzlich der PCSC-Dämon gestartet sein.

Achtung:

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

3.6 Der Lizenzschlüssel

Aufgabe des Lizenzschlüssels

Sollten Sie DATA Boreum über die Governikus KG erworben haben, ist ein Lizenzschlüssel für den Betrieb notwendig. Der Lizenzschlüssel steuert die Nutzungsdauer. Sie bekommen einen Lizenzschlüssel, wenn sie DATA Boreum im Onlineshop der Governikus KG erwerben. Der Lizenzschlüssel wird Ihnen dann per E-Mail zugeschickt. Ohne Lizenzschlüssel kann DATA Boreum als Demo-Version für 30 Tage verwendet werden. Wenn ein Lizenzschlüssel nur noch weniger als 40 Tage gültig ist, wird die Anzahl der verbleibenden Tage in DATA Boreum auf dem oberen Fensterrahmen angezeigt.

Eingabe des Lizenzschlüssels

Um den Lizenzschlüssel einzugeben, starten Sie DATA Boreum und wählen Sie im Menü "Hilfe" die Option "Lizenz". Dies öffnet die Dialogseite "DATA Boreum Lizenzschlüssel". Geben Sie den Lizenzschlüssel ein und schließen Sie die Eingabe mit OK ab.

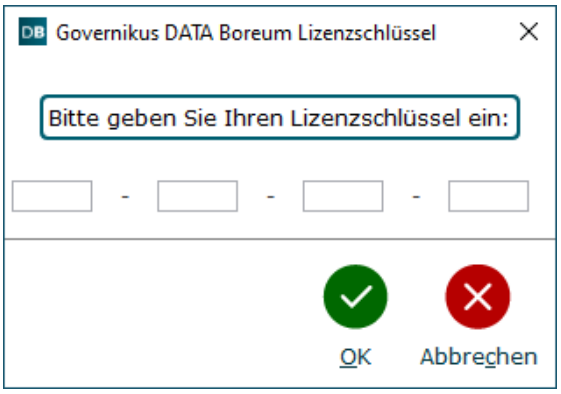

Abbildung 8: Dialogseite zur Eingabe des Lizenzschlüssels

	Achtung: Der Lizenzschlüssel wird erst nach einem Neustart von DATA Boreum wirksam.

Gültiger Lizenzschüssel: Wenn Sie einen gültigen Lizenzschlüssel eingegeben haben, wird das folgende Dialogfenster angezeigt.

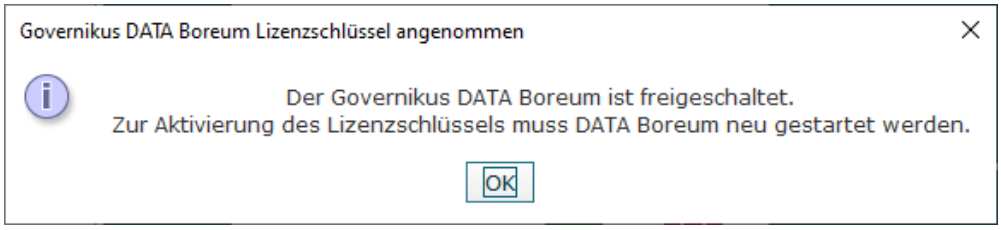

Abbildung 9: Aufforderung zum Neustart nach Lizenzschlüsseleingabe

Ungültiger Lizenzschlüssel: Wenn Sie einen ungültigen Lizenzschlüssel eingegeben haben, wird das folgende Dialogfenster angezeigt. Klicken Sie auf OK und geben Sie einen gültigen Lizenzschlüssel ein.

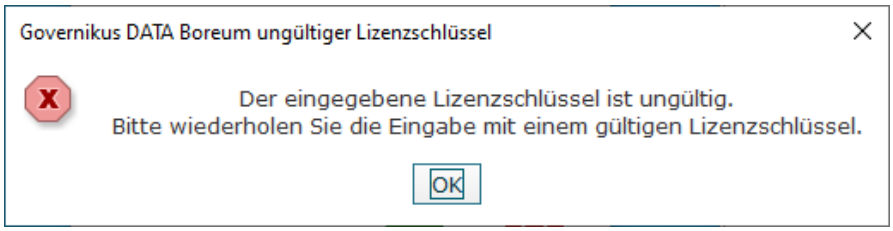

Abbildung 10: Warnhinweis bei ungültigem Lizenzschlüssel

4 Schnelleinstieg

Die folgenden Seiten bieten Ihnen einen Schnelleinstieg in die Funktionen von Governikus DATA Boreum. Die Bedienung von Governikus DATA Boreum ist einfach und überwiegend selbsterklärend. Alle Schritte sind in nachfolgenden Kapiteln erklärt, die Sie über die jeweiligen Kapitelreferenzen direkt anspringen können.

4.1 Schnelleinstieg Signieren

Klicken Sie auf der Einstiegsseite von Governikus DATA Boreum auf "Signieren", benutzen Sie alternativ das Tastaturkürzel "Strg + 1".

Dieses Tastaturkürzel ist bei macOS nicht anwendbar.

Nachdem Sie die Funktion Signieren gewählt haben, wird auf der linken Seite eine Buttonleiste zur Dialogseitenauswahl angezeigt. Klicken Sie nacheinander auf die Buttons, um dort Ihre Auswahl zu treffen.

1. **Dateiauswahl**: Wählen Sie die Dateien aus, die Sie signieren wollen. Sie können auch im Dateimanager eine Datei auswählen und aus dem Kontextmenü "Signieren" wählen. Ausführliche Erläuterungen finden Sie in Kapitel 6.4.1.
2. **Optionen**: Wählen Sie hier das Signaturformat. Ausführliche Erläuterungen finden Sie in Kapitel 6.4.3.
3. **Schlüssel wählen**: Wählen Sie hier Zertifikat und Schlüssel für Ihre elektronische Signatur. Ausführliche Erläuterungen finden Sie in Kapitel 6.4.4.
4. **Zielverzeichnis wählen**: Wählen Sie hier das Verzeichnis aus, in dem die elektronisch signierten Dateien abgelegt werden sollen. Ausführliche Erläuterungen finden Sie in Kapitel 6.4.5.
5. **Signieren**: Lösen Sie nach den oben vorgenommenen Einstellungen hier den Signiervorgang aus. Ausführliche Erläuterungen finden Sie in Kapitel 6.4.6.

4.2 Schnelleinstieg Validieren

Klicken Sie auf der Einstiegsseite von Governikus DATA Boreum auf "Validieren", benutzen Sie alternativ das Tastaturkürzel "Strg + 2".

Dieses Tastaturkürzel ist bei macOS nicht anwendbar.

Nachdem Sie die Funktion Validieren gewählt haben, wird auf der linken Seite eine Buttonleiste zur Dialogseitenauswahl angezeigt. Klicken Sie nacheinander auf die Buttons, um dort Ihre Auswahl zu treffen.

6. **Dateiauswahl**: Wählen Sie die Dateien aus, die Sie validieren wollen. Sie können auch im Dateimanager eine Datei auswählen und aus dem Kontextmenü "Validieren" wählen. Ausführliche Erläuterungen finden Sie in Kapitel 6.5.1.
7. **Optionen**: Wählen Sie hier, ob eine Online-Überprüfung stattfinden soll. Wählen Sie danach das Verzeichnis aus, in dem das Prüfprotokoll der Validierung abgelegt werden soll. Ausführliche Erläuterungen finden Sie in Kapitel 6.5.3.
8. **Validieren**: Lösen Sie nach den oben vorgenommenen Einstellungen hier die Validierung aus. Ausführliche Erläuterungen finden Sie in Kapitel 6.5.

4.3 Schnelleinstieg Verschlüsseln

Klicken Sie auf der Einstiegsseite von Governikus DATA Boreum auf "Verschlüsseln", benutzen Sie alternativ das Tastaturkürzel "Strg + 3".

Dieses Tastaturkürzel ist bei macOS nicht anwendbar.

Nachdem Sie die Funktion Verschlüsseln gewählt haben, wird auf der linken Seite eine Buttonleiste zur Dialogseitenauswahl angezeigt. Klicken Sie nacheinander auf die Buttons, um dort Ihre Auswahl zu treffen.

9. **Dateiauswahl**: Wählen Sie die Dateien aus, die Sie verschlüsseln wollen. Sie können auch im Dateimanager eine Datei auswählen und aus dem Kontextmenü "Verschlüsseln" wählen. Ausführliche Erläuterungen finden Sie in Kapitel 6.6.1.
10. **Schlüssel wählen**: Wählen Sie hier den öffentlichen Schlüssel der Personen aus, für die Sie die Datei verschlüsseln wollen. Ausführliche Erläuterungen finden Sie in Kapitel 6.6.2.
11. **Zielverzeichnis wählen**: Wählen Sie hier das Verzeichnis aus, in dem die verschlüsselten Dateien abgelegt werden sollen. Ausführliche Erläuterungen finden Sie in Kapitel 6.6.3.
12. **Verschlüsseln**: Lösen Sie nach den oben vorgenommenen Einstellungen hier den Verschlüsselungsvorgang aus. Ausführliche Erläuterungen finden Sie in Kapitel 6.6.4.

4.4 Schnelleinstieg Entschlüsseln

Klicken Sie auf der Einstiegsseite von Governikus DATA Boreum auf "Entschlüsseln", benutzen Sie alternativ das Tastaturkürzel " Strg + 4".

Dieses Tastaturkürzel ist bei macOS nicht anwendbar.

Nachdem Sie die Funktion Entschlüsseln gewählt haben, wird auf der linken Seite eine Buttonleiste zur Dialogseitenauswahl angezeigt. Klicken Sie nacheinander auf die Buttons, um dort Ihre Auswahl zu treffen.

13. **Dateiauswahl**: Wählen Sie die Dateien aus, die Sie entschlüsseln wollen. Sie können auch im Dateimanager eine Datei auswählen und aus dem Kontextmenü "Entschlüsseln" wählen. Ausführliche Erläuterungen finden Sie in Kapitel 6.7.1.
14. **Schlüssel wählen**: Wählen Sie hier Ihren privaten Schlüssel aus, der zum öffentlichen Schlüssel passt, mit dem die Datei verschlüsselt wurde. Ausführliche Erläuterungen finden Sie in Kapitel 6.7.2.
15. **Zielverzeichnis wählen**: Wählen Sie hier das Verzeichnis aus, in dem die entschlüsselten Dateien abgelegt werden sollen. Ausführliche Erläuterungen finden Sie in Kapitel 6.7.3.
16. **Entschlüsseln**: Lösen Sie nach den oben vorgenommenen Einstellungen hier den Entschlüsselungs-vorgang aus. Ausführliche Erläuterungen finden Sie in Kapitel 6.7.4.

5 Einstellungen

Sie können diesen Dialog über das Menü "Extras" und die Option "Einstellungen" aufrufen. Der Dialog "Einstellungen" enthält mehrere Registerkarten, die im Folgenden erklärt werden. Auf jeder Registerkarte im "Einstellungen"-Dialog finden Sie diese Buttons:

- **Speichern**: Über diesen Button speichern Sie Ihre Einstellungen. Wenn Sie Änderungen auf verschiedenen Registerkarten des "Einstellungen"-Dialogs vorgenommen haben, reicht es aus, diesen Button einmal für alle Änderungen zu benutzen. Mit dem Speichern-Button verlassen Sie den "Einstellungen"-Dialog.

	Hinweis: Bitte beachten Sie, dass dieser Button in der Governikus DATA Boreum Integration Edition mit "Vorübergehend übernehmen" beschriftet ist und eine andere Bedeutung hat. Bitte lesen Sie dazu Kapitel 8.

- **Abbrechen**: Mit diesem Button verlassen Sie den "Einstellungen"-Dialog, ohne dass eventuell vorgenommene Änderungen gespeichert werden. Alle nach dem letzten Speichern vorgenommen Änderungen von allen Registerkarten gehen verloren.
- **Hilfe**: Mit diesem Button rufen Sie die Online-Hilfe von Governikus DATA Boreum auf.

Allgemeine Tastaturbefehle im Dialog Einstellungen

- Strg + s = Konfiguration speichern und Dialogfenster schließen (Dieses Tastaturkürzel ist bei macOS nicht anwendbar.)
- Esc = Abbrechen
- F1 = Hilfe

5.1 Registerkarte Allgemein

Diese Registerkarte bietet Ihnen die folgenden Einstellungsmöglichkeiten.

- **Protokollierung**: Wenn Sie diese Option auswählen, müssen Sie anschließend über den Button "Protokollverzeichnis wählen" ein Verzeichnis auswählen, in dem die Protokolldateien abgelegt werden. Diese Protokolldateien enthalten Fehler und Ausnahmezustände, die während der Programmausführung aufgetreten sind. Ihre PIN und andere sicherheitsrelevante Eingaben werden natürlich nicht protokolliert. Nach der Auswahl des Protokollverzeichnisses wird der Pfad im nebenstehenden Eingabefeld angezeigt. Sie können den Pfad auch direkt in dieses Eingabefeld eingeben. Sollte das angegebene Verzeichnis nicht existieren, wird es angelegt. Bei jedem Programmstart wird eine Protokolldatei im angegebenen Verzeichnis erstellt, die den Namen `<Erstellungsdatum>_DATABoreum_<Versionsnummer>.log` hat. Dabei ist `<Erstellungsdatum>` das Datum und die Uhrzeit des Governikus DATA Boreum Programmstarts und `<Versionsnummer>` ist die Version von Governikus DATA Boreum.

Die folgende Abbildung zeigt den Dialog Einstellungen mit der Registerkarte Allgemein.

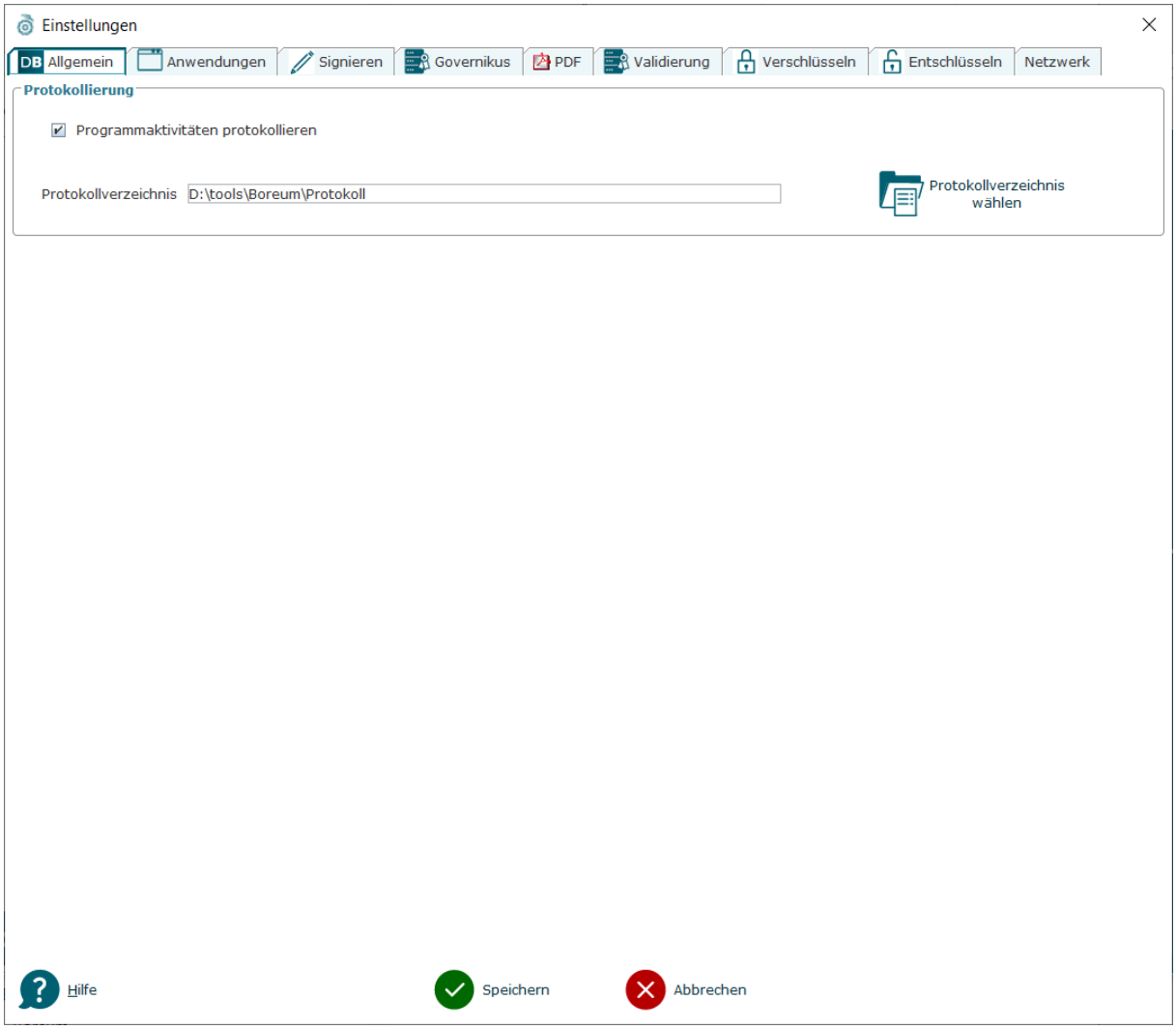

Abbildung 11: Registerkarte Allgemein im Einstellungsdialog

Tastaturbefehle auf dieser Seite

- Alt + w = Protokollverzeichnis wählen

Dieses Tastaturkürzel ist bei macOS nicht anwendbar.

5.2 Registerkarte Anwendungen

In dieser Registerkarte können Sie Programme konfigurieren, die am Ende einer Governikus DATA Boreum Funktion ausgeführt werden können. Auf der letzten Dialogseite der Governikus DATA Boreum Funktionen "Signieren", "Validieren", "Verschlüsseln" und "Entschlüsseln" wird die Möglichkeit geboten, aus einer Liste eines der hier konfigurierten Programme auszuwählen. Die Ergebnisdateien, die auf dieser letzten Dialogseite erstellt werden, werden direkt an das ausgewählte und hier konfigurierte Programm übergeben und können dann mit diesem Programm weiterverarbeitet werden. Die folgende Auswahl steht immer zur Verfügung:

- **Keine Weiterverarbeitung**: Governikus DATA Boreum führt keine Aktion nach dem Abschluss der ausgewählten Funktion aus.

- **Signieren**: Nach Ausführung der ausgewählten Funktion werden die Dateien an die Funktion Signieren übergeben. Steht nicht in der Funktion Signieren zur Verfügung.
- **Validieren**: Nach Ausführung der ausgewählten Funktion werden die Dateien an die Funktion Validieren übergeben. Steht nicht in der Funktion Validieren zur Verfügung, ist nur sinnvoll nach dem Signieren.
- **Verschlüsseln**: Nach Ausführung der ausgewählten Funktion werden die Dateien an die Funktion Verschlüsseln übergeben. Steht nicht in der Funktion Verschlüsseln zur Verfügung.
- **Entschlüsseln**: Nach Ausführung der ausgewählten Funktion werden die Dateien an die Funktion Entschlüsseln übergeben. Steht nicht in der Funktion Entschlüsseln zur Verfügung, ist nur sinnvoll nach dem Verschlüsseln.
- **E-Mail**: Nach Ausführung der ausgewählten Funktion werden die Dateien an das Programm auf Ihrem Computer übergeben, das zum Versenden von E-Mails registriert ist.
- **Drucken**: Nach Ausführung der ausgewählten Funktion werden die Dateien an den Standarddrucker übergeben. Dies ist nur möglich, wenn für den Dateityp eine Verknüpfung mit dem Druckprogramm existiert. Ob eine Verknüpfung des Dateityps mit dem Druckprogramm vorhanden ist, können Sie überprüfen, indem Sie im Datei-Explorer Ihres Rechners die Datei auswählen und das Kontextmenü öffnen. Ist dort die Option "Drucken" aufgeführt, existiert eine Verknüpfung.
- **Öffnen**: Nach Ausführung der ausgewählten Funktion werden die Dateien an jeweils das Programm übergeben, dass auf Ihrem Rechner mit der jeweiligen Dateiendung verbunden ist. Wenn keine Verbindung mit einem Programm auf Ihrem Rechner existiert, wird eine Auswahlmöglichkeit angezeigt.

Weitere Anwendungen

Klicken Sie auf den Button "Anwendung verwalten", um Programme hinzuzufügen, zu bearbeiten oder zu entfernen. Es wird dieser Dialog angezeigt:

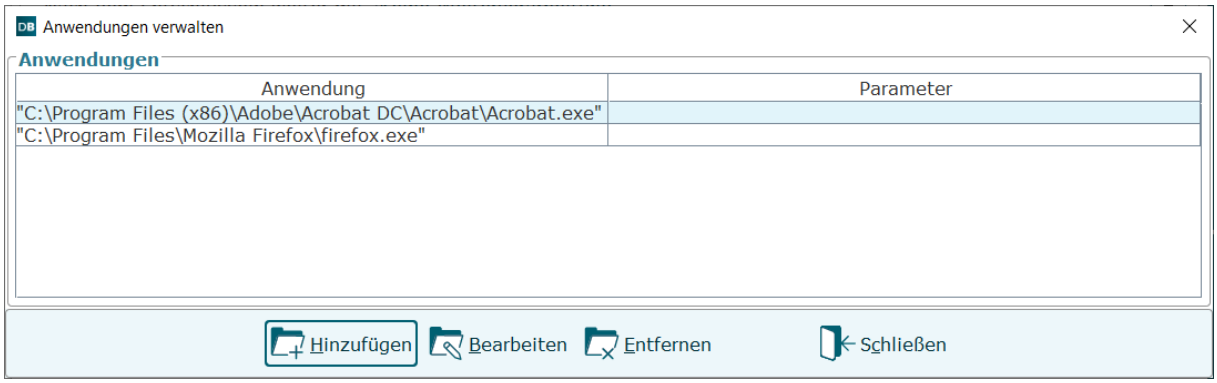

Abbildung 12: Programme verwalten

Bitte beachten Sie, dass bei einem macOS nur die Funktionen zur Verfügung stehen, die im vorangegangenen Abschnitt beschrieben sind. Die Übergabe von Dateien an Programme, die in "Anwendungen verwalten" angegeben werden können, funktioniert bei einem macOS nicht.

Tastaturbefehle auf der Dialogseite "Anwendungen verwalten"

- Alt + a = Hinzufügen, Alt + b = Bearbeiten, Alt + e = Entfernen

- Entf = Entfernen
- Alt + s = Schließen
- Esc = Schließen

Sie können nun entweder die Einstellungen zu einem bereits aufgelisteten Programm bearbeiten oder ein neues Programm hinzufügen.

- Zum Editieren wählen Sie ein Programm aus der Liste aus und klicken Sie auf den Bearbeiten-Button. Es wird der Dialog "Anwendung verwalten" mit den aktuellen Einstellungen angezeigt.
- Wenn Sie ein Programm hinzufügen wollen, wird derselbe Dialog aufgerufen, allerdings ohne Vorbelegung.

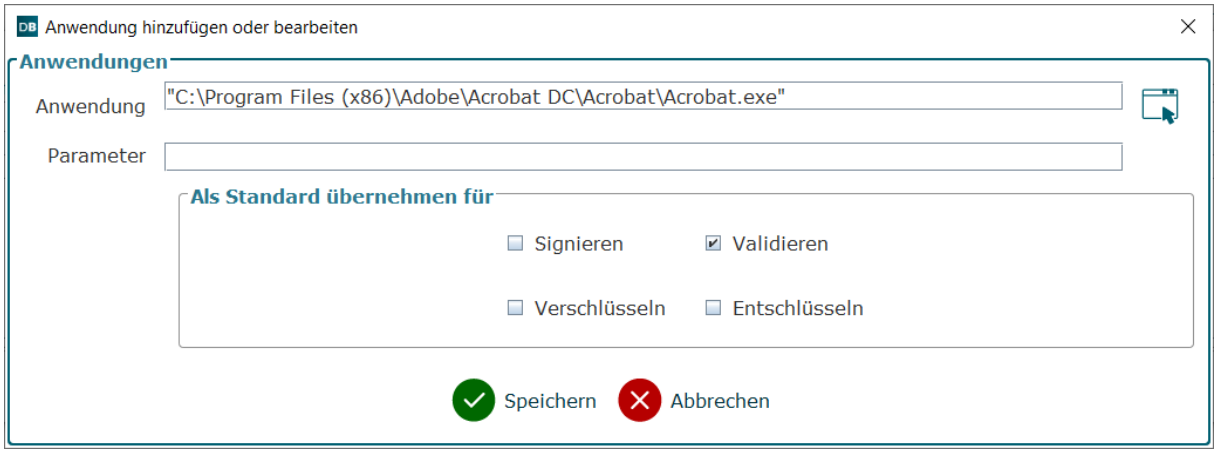

Abbildung 13: Programm hinzufügen oder bearbeiten

Über das grüne "Plus" Symbol am Ende der Zeile "Anwendung" können Sie zu der ausführbaren Datei des Programms navigieren, das Sie hinzufügen wollen. Der Pfad und die Datei werden danach im Feld "Anwendung" angezeigt. Ergänzen Sie anschließend evtl. erforderliche Aufrufparameter in dem Feld Parameter. Welche Parameter Sie in welcher Syntax hinzufügen müssen, ist abhängig vom ausgewählten Programm. Lassen Sie sich nötigenfalls diese Einstellungen von Ihrem Systemadministrator nennen.

Tastaturbefehle auf der Dialogseite "Anwendungen hinzufügen oder verwalten"

- Alt + o = Dateiauswahl öffnet sich, um eine Anwendung auswählen zu können
- Enter = OK
- Esc = Abbrechen

Die folgende Abbildung zeigt die Registerkarte "Anwendungen" im Dialog Einstellungen.

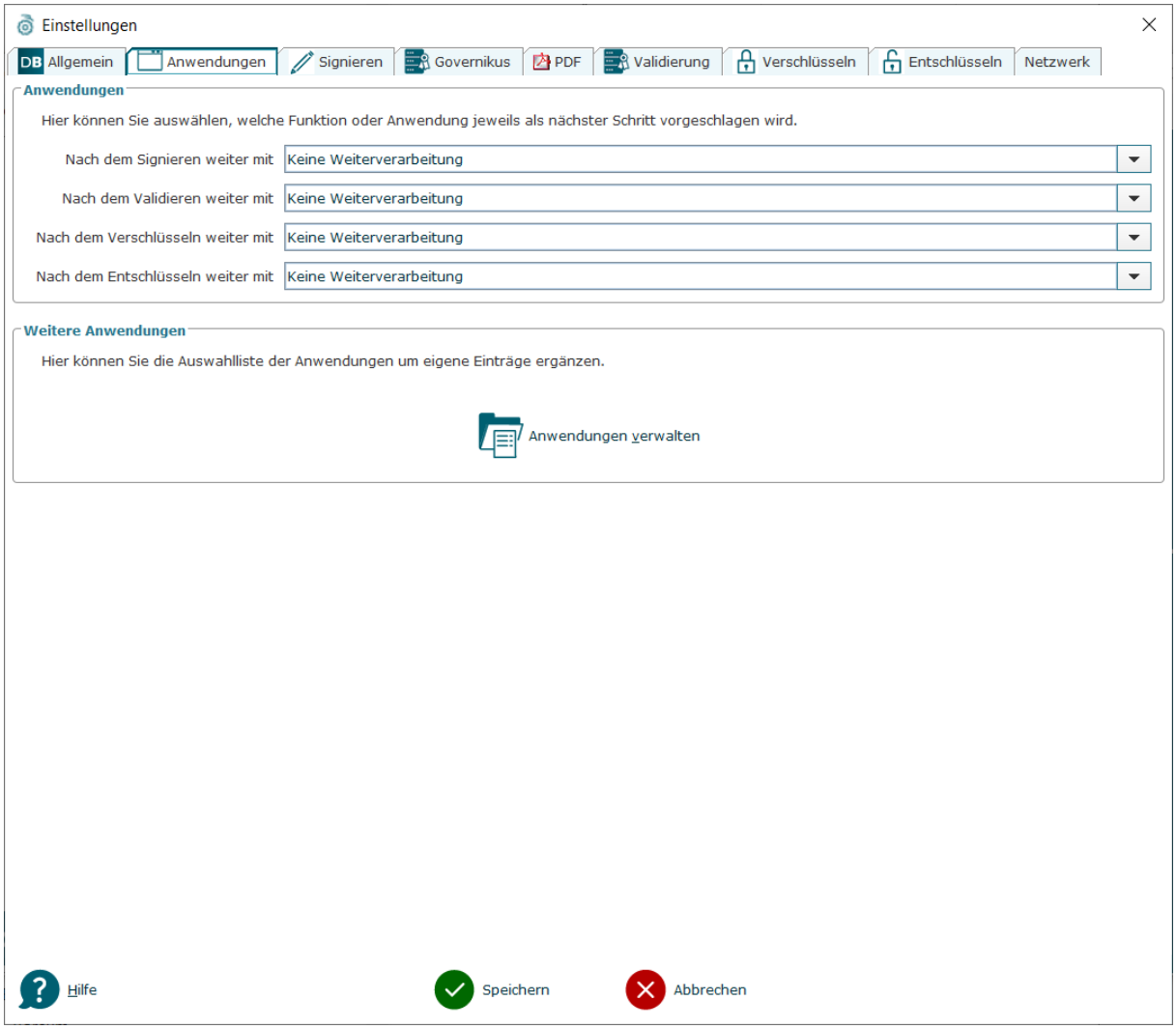

Abbildung 14: Registerkarte Anwendungen

Tastaturbefehle auf dieser Seite

- Alt + v = Dialogseite "Anwendungen verwalten" aufrufen

5.3 Registerkarte Signieren

Auf dieser Registerkarte finden Sie die folgenden Einstellungen:

Anzahl der einzusehenden Dateien

Nach ETSI EN 319 102 muss eine Software, mit der Dateien elektronisch signiert werden können, die Möglichkeit bieten, die Dateien vor dem Signieren anzuschauen.

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

zusammengestellten Dateien in der Dateiliste vertrauen, können Sie hier eine Zahl zwischen 1 und 100 angeben.

Quelldateien löschen

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

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

Unterschiedliche Signaturformate werden in Kapitel 9.4 erklärt. Die Quell-Dateien werden erst nach dem erfolgreichen Signieren gelöscht. **Hinweis**: Die Dateien werden endgültig gelöscht. Es existieren danach nur noch die signierten Dateien. Die folgende Abbildung zeigt die Registerkarte "Signieren" im Dialog Einstellungen.

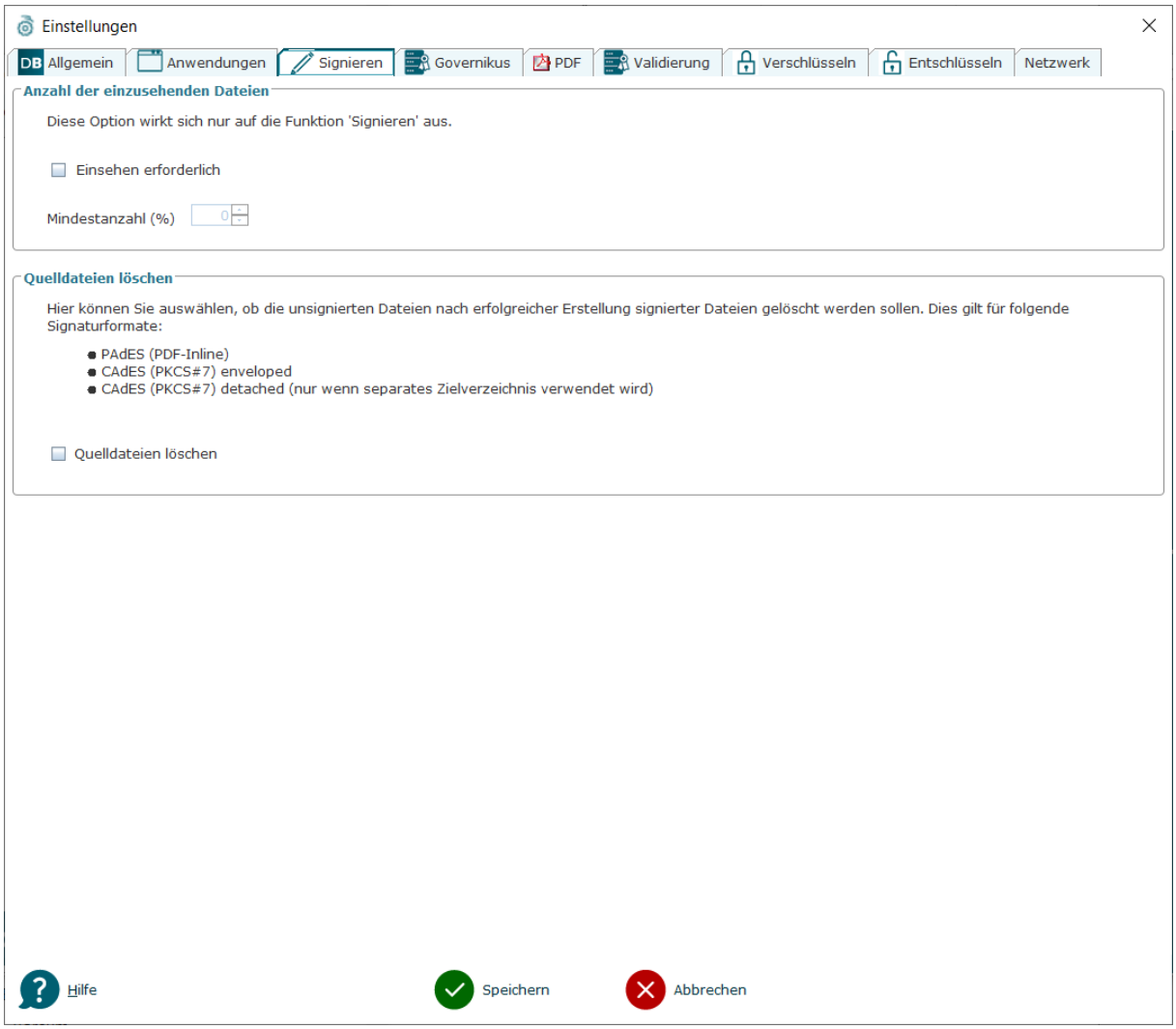

Abbildung 15: Registerkarte Signieren

5.4 Registerkarte Governikus

Die Konfiguration auf der hier beschriebenen Dialogseite bezieht sich auf die Dienste, die DATA Boreum bei der Serversoftware Governikus Suite nutzen kann. Die Governikus Suite enthält das Produkt DATA Deneb, dem DATA Boreum Dateien zur Massensignatur übergeben kann und von dem DATA Boreum auch Zeitstempel beziehen kann.

Sie müssen daher auf dieser Dialogseite von DATA Boreum **nur dann** Daten eintragen, wenn Sie den Signaturdienst von DATA Deneb für Massensignaturen nutzen wollen oder wenn Sie für Signaturen einen Zeitstempel von DATA Deneb anfordern möchten.

Damit die Dienste des Produkts DATA Deneb nur von befugten Clients angefragt werden können, muss DATA Boreum sich gegenüber der Serversoftware authentifizieren. Daher müssen auf dieser Dialogseite auch die Daten für den Authentisierungsdienst angegeben werden.

Hinweis: Die konkreten Verbindungs- und Konfigurationsdaten, die Sie auf dieser Dialogseite benötigen, erhalten Sie vom Administrator der Governikus Suite.

Authentisierungsdienst

DATA Boreum muss im Authentisierungsdienst als Client konfiguriert sein, damit DATA Boreum Anfragen an die Dienste von DATA Deneb stellen kann. Die Anfragen werden vom Authentisierungsdienst authentisiert und zu den entsprechenden Diensten weitergeleitet. Hier wird die Authentifizierung geprüft und danach wird die Anfrage vom Dienst ausgeführt. Für die Konfiguration des Authentisierungsdiensts in DATA Boreum müssen die folgen Daten angegeben werden:

- **Server**: Geben Sie hier die Adresse des Authentisierungsdiensts als URL an. Ersetzen Sie im Beispiel `<server>` durch den korrekten Servernamen oder die IP-Adresse:
  - `https://<server>:8443/auth` **Hinweis**: bitte beachten Sie, dass die Pfadangabe `/auth` in der URL nur für Authentisierungsserver (Keycloak) in der Version 16.x oder älter genutzt werden darf, bei späteren Version muss diese Erweiterung entfallen, also:
  - `https://<server>:8443/` nehmen Sie diese URL für Authentisierungsserver (Keycloak) in der Version 17.0.1 oder jünger
- **Realm-Name**: Dieser Name bezeichnet die gültige Konfiguration für den Authentisierungsdienst. Dieser Eintrag lautet in der Standardeinstellung wie folgt: `governikus-extern`
- **Client ID**: Unter diesem Namen ist DATA Boreum als Client im Authentisierungsdienst angelegt. Dieser Eintrag lautet in der Standardeinstellung wie folgt: `boreum-client`
- **Client Secret**: Hier muss eine Zeichenkette aus Buchstaben und Zahlen eingegeben werden, die den Client im Authentisierungsdienst eindeutig identifiziert.

Signaturdienst

Über den Signaturdienst ist DATA Boreum in der Lage, Massensignaturen an bis zu 500 Dateien in einem Aufruf zu erstellen. Für die Konfiguration des Signaturdienstes in DATA Boreum muss die Serveradresse als URL angegeben werden:

- **Server**: Geben Sie hier die Adresse des Signaturdienstes als URL an. Ersetzen Sie im Beispiel `<server>` durch den korrekten Servernamen oder die IP-Adresse:

- `https://<server>:8443/signservice/rest`

Zeitstempeldienst

Mit dem Zeitstempeldienst ist DATA Boreum in der Lage, Zeitstempel zu den Signaturen von Dateien hinzuzufügen. Für die Konfiguration des Zeitstempeldiensts in DATA Boreum müssen die folgen Daten angegeben werden:

- **Server**: Geben Sie hier die Adresse des Zeitstempeldiensts als URL an. Ersetzen Sie im Beispiel `<server>` durch den korrekten Servernamen oder die IP-Adresse:

  - `https://<server>:8443/timestampservice/rest`

- **Profil-ID**: Mit der Profil-ID wird ein konkreter Zeitstempeldienst angesprochen, von dem die qualifizierten, elektronischen Zeitstempel angefordert werden können. Die Profil-ID muss genau so geschrieben werden, wie Sie in der Governikus Suite hinterlegt ist. Groß- und Kleinschreibung wird unterschieden.

Die folgende Abbildung zeigt die Registerkarte Governikus mit einer Beispielbelegung.

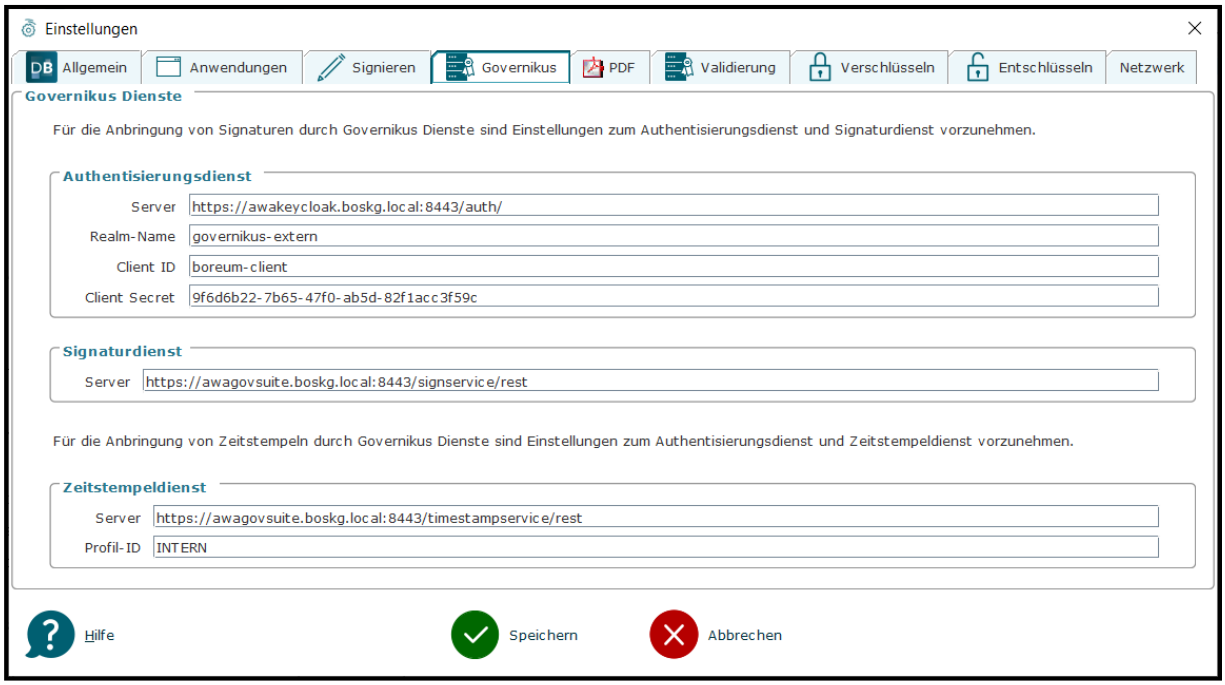

Abbildung 16: Registerkarte Governikus

5.5 Registerkarte BNotK

BNotK ist die Abkürzung für Bundesnotarkammer. Auf der Registerkarte BNotK können Sie die Benutzung des Fernsignaturdienstes der BNotK ein- und ausschalten. Damit Sie diese Funktion benutzen können, setzen Sie einen Haken in die Checkbox „Ja, der Fernsignaturdienst soll verwendet werden“.

Voraussetzung für die Benutzung des Fernsignaturdienstes der BNotK ist eine Authentisierungskarte der BNotK, die dazugehörige PIN und einen Chipkartenleser.

Wenn die Checkbox auf dieser Registerkarte ausgewählt ist,

- werden automatisch die Konfigurationsparameter in Dialogabschnitt „Konfiguration“ angezeigt. Diese Angaben sind nicht editierbar.
- wird in der Funktion „Signieren“ auf der Dialogseite „Schlüssel wählen“ unter „Speicherort des Schlüssels“ der Button „BNotK Fernsignaturdienst“ angezeigt. Das benötigte Authentisierungszertifikat wird nach dem Einlegen der Authentisierungskarte der BNotK und der Eingabe der PIN angezeigt.
- wird ein möglicherweise zuvor angezeigter Button mit einem Chipkartenleser zum Signieren mit Signaturkarte nicht mehr angezeigt. Zum Signieren mit Signaturkarte muss zuvor die Checkbox auf dieser Registerkarte wieder abgewählt werden.

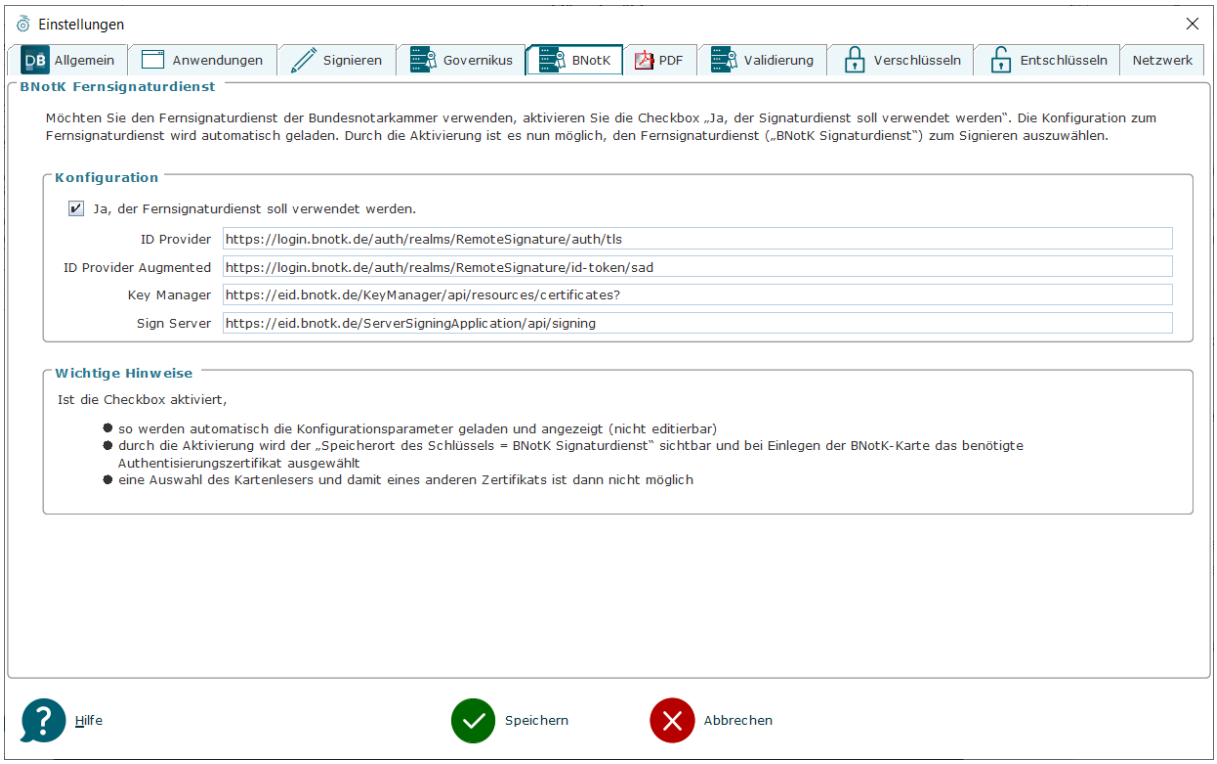

Abbildung 17: Registerkarte BNotK

5.6 Registerkarte PDF

Die Einstellungen, die Sie hier vornehmen können, werden nur wirksam, wenn Sie bei der Funktion Signieren (vgl. Kapitel 6.4.3) auf der Dialogseite "Optionen" die Einstellung "PDF-Signatur erstellen" ausgewählt haben. PDF-Dokumente bieten die Möglichkeit, zusätzlich zur eigentlichen Signatur sicht- und druckbare Signaturinformationen im Dokument aufzunehmen. Die Registerkarte PDF ist in mehrere Dialogabschnitte unterteilt, die im Folgenden erklärt werden.

Dialogabschnitt „Soll ein Signaturfeld sichtbar sein?

Bitte beachten Sie unbedingt, dass sich die Einstellungen, die Sie hier vornehmen, auf **alle** PDF-Signaturen auswirken, so wie Sie diese auf der Dialogseite „Optionen“ konfiguriert haben, lesen Sie dazu Kapitel 6.4.3.2.

- **Unsichtbares Signaturfeld**: Wenn Sie diese Option wählen, wird kein sichtbares Signaturfeld angelegt. Die Signatur wird nur in der PDF-Datei im Bereich "Unterschriften" angezeigt.
- **Sichtbares Signaturfeld**: Es wird ein sichtbares Signaturfeld angelegt, dessen Erscheinungsbild Sie in den folgenden Dialogabschnitten festlegen können.

Wenn Sie „Sichtbares Signaturfeld“ ausgewählt haben, werden **alle** Einträge der nachfolgen Dialogabschnitte wirksam.

	**Hinweis**: Auch wenn Sie die Option „Sichtbares Signaturfeld“ auswählen, aber die nachfolgenden Dialogabschnitte nicht konfigurieren, wird ein sichtbares Signaturfeld mit den vorhandenen Standardeinstellungen erstellt.

- **Art**: Hier wählen Sie aus, ob die Darstellung Text (zusätzliche Unterschriftsinformationen), eine Grafik oder beides enthalten soll.
- **Layout**: Wenn Sie im Feld "Art" die Option "Text und Grafik" ausgewählt haben, können Sie hier auswählen, wie Grafik und Text zueinander angeordnet werden sollen.
- **Grafik/Text**: Hier können Sie das Größenverhältnis zwischen Grafik und Text auswählen.
- **Vorlage**: Über den Button „Vorlage“ können Sie Einstellungen für die PDF-Signatur als Vorlagen verwalten. Dies ist im folgenden Kapitel erklärt.

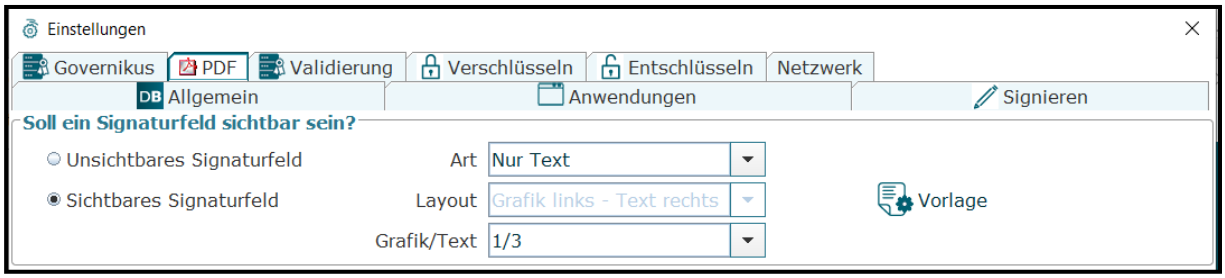

Abbildung 18: Dialogabschnitt "Soll ein Signaturfeld sichtbar sein?"

5.6.1 Vorlagen verwalten

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

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

Vorlagennamen auswählbar. **Hinweis**: Wählen Sie einen möglichst sprechenden Namen für eine Vorlage, damit daraus die dahinterstehende Konfiguration klar wird.

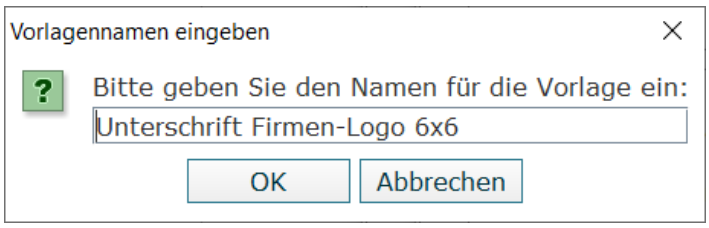

Abbildung 19: Vorlagennamen eingeben

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

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

Abbildung 20: Vorlagen verwalten mit Beispielvorlagen

5.6.2 Visualisierung

Zusätzliche Unterschriftsinformationen

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

- **Unterzeichner:in:** Wählen Sie hier, wie Ihre persönlichen Daten angezeigt werden:
  - **Aus Signaturzertifikat entnehmen**: Wenn Sie diese Option wählen, wird bei jeder Signatur der Name aus dem Signaturzertifikat verwendet.
  - **Name**: Wenn Sie diese Option wählen, können Sie einen abweichenden Namen (z. B. mit abgekürztem Vornamen) mit maximal 50 Zeichen eintragen oder, wenn Sie keinen Unterzeichner angeben möchten, das Feld leer lassen.
- **Datum**: Wenn Sie die Checkbox auswählen, wird das aktuelle Datum als zusätzliche Information in der Visualisierung dargestellt. Bitte beachten Sie, dass in der Signatur selbst der Signaturzeitpunkt immer enthalten ist.
- **Formatierung**: Unter "Formatierung" können Sie die Darstellungsform des Datums verändern.

Zu den zusätzlichen Unterschriftsinformationen gehören auch der Ort und der Unterschriftsgrund. Die Eingabe des Ortes und des Grundes erfolgt direkt im Dialog "Signieren" im Schritt "Optionen". Dies wird sowohl für sichtbare als auch unsichtbare Signaturen übernommen.

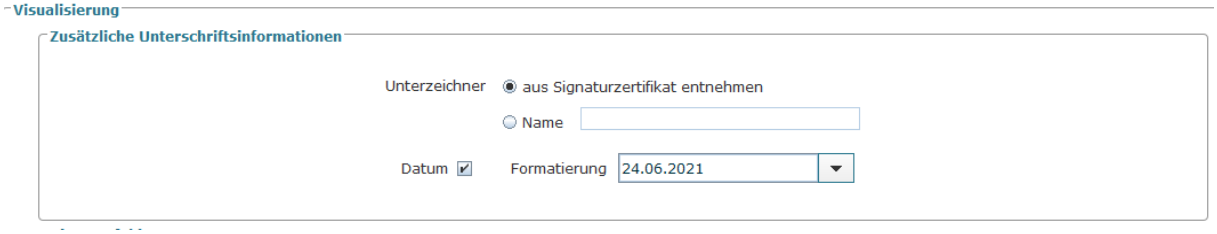

Abbildung 21: Dialogabschnitt "Zusätzliche Unterschriftsinformationen"

5.6.3 Signaturfeld platzieren

Ein Signaturfeld erstellen, falls dieses nicht vorhanden ist

Entscheiden Sie in diesem Dialogabschnitt als erstes über diese Option:

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

- In dem PDF-Dokument, das signiert werden soll, wurde kein sichtbares Signaturfeld angelegt. In diesem Fall wird eine unsichtbare Signatur eingefügt.

- **Ausgewählt**: Wenn diese Option ausgewählt ist, wird ein sichtbares Signaturfeld erstellt, wenn noch kein anderes sichtbares Signaturfeld vorher erstellt wurde oder alle sichtbaren Signaturfelder bereits belegt sind.

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

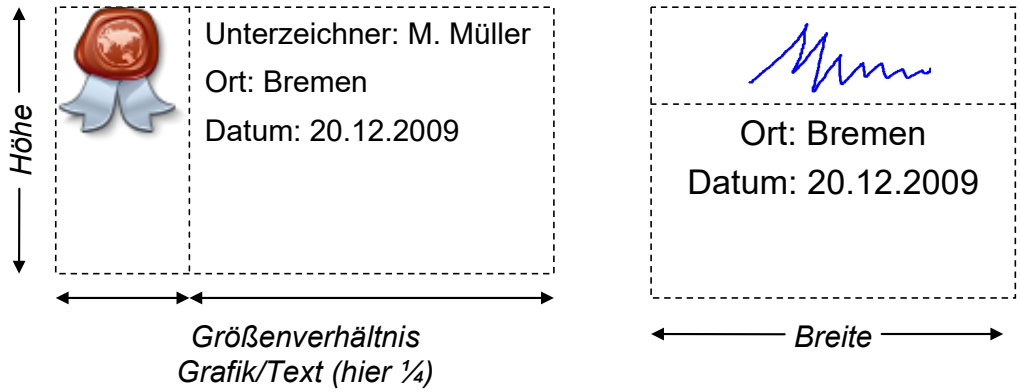

Abbildung 22: Beispiele für eine Visualisierung mit Grafik und Text

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

Seite: Wählen Sie hier aus, ob die Darstellung auf der ersten oder auf der letzten Seite des Dokumentes erfolgen soll.

Breite: Bestimmen Sie hier, welche Breite die sichtbaren Signaturinformationen überdecken sollen.

Höhe: Bestimmen Sie hier, welche Höhe die sichtbaren Signaturinformationen überdecken sollen.

Position: Legen Sie fest, an welcher Position auf der Dokumentenseite die sichtbaren Signaturinformationen dargestellt werden sollen. Halten Sie dazu den roten Rahmen mit der Maus fest und ziehen Sie ihn an die Position, an der die Visualisierung auf der Seite angezeigt werden soll.

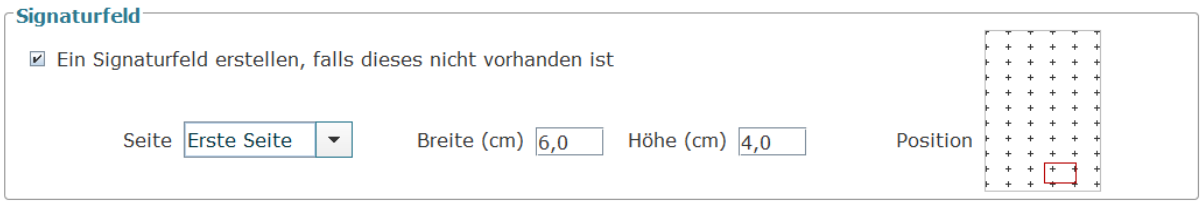

Abbildung 23: Dialogabschnitt "Signaturfeld platzieren"

5.6.4 Schrift

Hier können Sie Details zu der Textdarstellung einstellen.

- **PDF/A kompatibel**: Soll die PDF/A Kompatibilität des PDF-Dokuments auch mit einer sichtbaren Signatur erhalten bleiben, wählen Sie bitte diese Option aus. Damit ist die individuelle Auswahl von Schriftart und Schriftfarbe nicht mehr möglich.
- **Schriftart**: Da die Darstellung des Dokuments auf unterschiedlichen Systemen möglich sein muss, ist die Auswahl der Schriftarten auf die Standardschriftarten "Times New Roman", "Helvetica" und "Courier New" beschränkt.
- **Schriftfarbe**: Wählen Sie aus der Drop-down-Liste die Schriftfarbe aus.
- **Schriftgröße**: Wählen Sie hier die Größe der Schrift aus.
- **automatisch verkleinern**: Ist die Checkbox unter "Schriftgröße" aktiviert, wird die Schriftgröße automatisch verkleinert, sofern der Text nicht in den definierten Platz passt
- **Formatierung**: Wählen Sie aus der Drop-down-Liste die Ausrichtung der Schrift aus.

5.6.5 Grafik

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

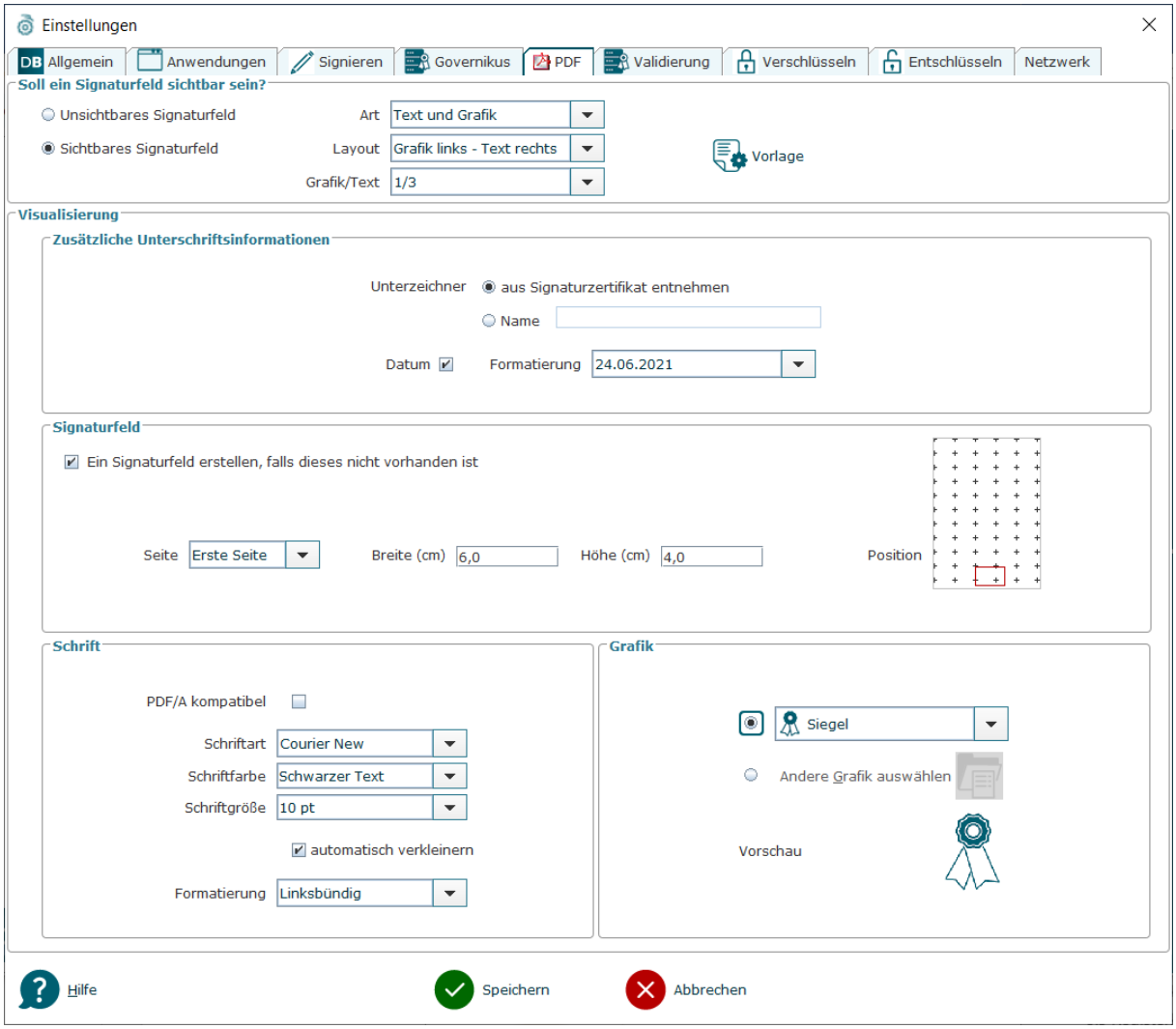

Abbildung 24: Registerkarte PDF im Dialog "Einstellungen"

5.7 Registerkarte Validierung

Format des Prüfprotokolls

Hier können Sie entscheiden, ob das Prüfprotokoll, das beim Validieren von Dateien entsteht, als HTML-, PDF- oder XML-Datei erstellt wird.

- **HTML**: Das Prüfprotokoll kann in einem Browser angezeigt werden.
- **PDF**: Das Prüfprotokoll kann in einem beliebigen PDF-Reader angezeigt werden.
- **XML**: Das Prüfprotokoll im XML-Format kann beispielsweise einer automatischen Auswertungssoftware oder einer Langzeitaufbewahrung übergeben werden.

Validierungsdienst

Mit der Funktionalität "Validieren" von Governikus DATA Boreum prüfen Sie, ob eine elektronisch signierte Datei unversehrt ist (Integrität) und die Signatur wirklich von der angegebenen Person ist (Authentizität). Zudem wird geprüft ob das Signaturzertifikat zum Zeitpunkt der Signaturerstellung gültig war. Dieser Vorgang ist auch im Kapitel 6.5 "Validieren" erklärt.

Für die Validierung muss sich Governikus DATA Boreum mit einem Validierungsdienst verbinden. Der Validierungsdienst übernimmt diese Validierung. Der Validierungsdienst ist Teil der Governikus Suite. Die Verbindungsdaten erhalten Sie von Ihrem Administrator, siehe unten. Die Angaben für die folgenden Felder werden von Ihrem Governikus Administrator ausgegeben:

- **Servername**: Geben Sie hier die URL zum Validierungsdienst an. Die URL hat diesen Aufbau: `https://<server>:8443//CertificateValidationServer/cvs`. Dabei ist `<server>` der Name des Servers auf dem der Validierungsdienst betrieben wird.
-  **Aktuell gültiges und zukünftig gültiges Zertifikat**: Mit dem hier hinterlegten Zertifikat wird die Integrität der Signatur geprüft, mit der die Antwort des Validierungsdienstes signiert ist. Damit ist gewährleistet, dass die Antwort auch wirklich von dem Validierungsdienst kommt, den Sie auf dieser Registerkarte konfiguriert haben. Zertifikate müssen rechtzeitig vor dem Ablauf ihrer Gültigkeitszeit ausgetauscht werden. Sind keine gültigen Zertifikate vorhanden schlägt die Signaturprüfung der Antwort fehl, die vom Validierungsdienst kommt.
  - **Aktuell gültiges Zertifikat**: Laden Sie hier das aktuell gültige Zertifikat hoch, siehe nächster Aufzählungspunkt "Zertifikat aus Datei laden".
  - **Zukünftig gültiges Zertifikat**: In der Zeile "Das zukünftig gültige Zertifikat" können Sie ein weiteres Zertifikat hochladen, das das bislang gültige Zertifikat in der Zukunft ablösen wird.

	**Hinweis**: Der Validierungsserver (Certificate Validation Server - CVS) erlaubt die Hinterlegung mehrerer Zertifikate, daher ist ein rechtzeitiger Austausch des Zertifikats nicht mehr notwendig. Nicht mehr benötigte Zertifikate, die nicht mehr im CVS hinterlegt sind, können gelöscht werden.

-  **Zertifikat aus Datei laden**: Klicken Sie auf das Ordnersymbol und navigieren Sie zu dem Verzeichnis, das die Datei mit dem Zertifikat enthält. Dieses Zertifikat wird Ihnen vom Governikus Administrator zur Verfügung gestellt. Die Datei muss die Dateiendung `.cer` oder `.crt` haben. **ACHTUNG**: Wenn bereits ein Zertifikat hochgeladen ist, wird es durch das neue Zertifikat ohne vorherige Warnung überschrieben.
-  **Zertifikat anzeigen**: Über den Button mit dem Lupe-Symbol wird das Zertifikat in einem separaten Fenster angezeigt. Dieser Button kann nur ausgewählt werden, wenn ein Zertifikat geladen wurde. Nachdem ein Zertifikat geladen wurde, ist dieser Button mit dem Namen des Zertifikatsinhabers beschriftet.
  - Die Zertifikatsanzeige können Sie entweder mit dem OK Button  schließen oder
  - das angezeigte Zertifikat 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.

- **Abbrechen** : Wenn Sie den Abbrechen-Button benutzen, wird der Dialog geschlossen. Sollten Sie Änderungen an der Konfiguration vorgenommen haben, werden diese verworfen.
- **Speichern** : Wenn Sie den Speichern-Button klicken, werden zuerst die angegebenen Verbindungsdaten geprüft. Wenn mit der vorliegenden Konfiguration eine Verbindung erstellt werden kann, werden die Verbindungsdaten gespeichert und der Dialog wird geschlossen.

Die folgende Abbildung zeigt die Dialogseite "Registerkarte Validierung" mit einer Beispielbelegung.

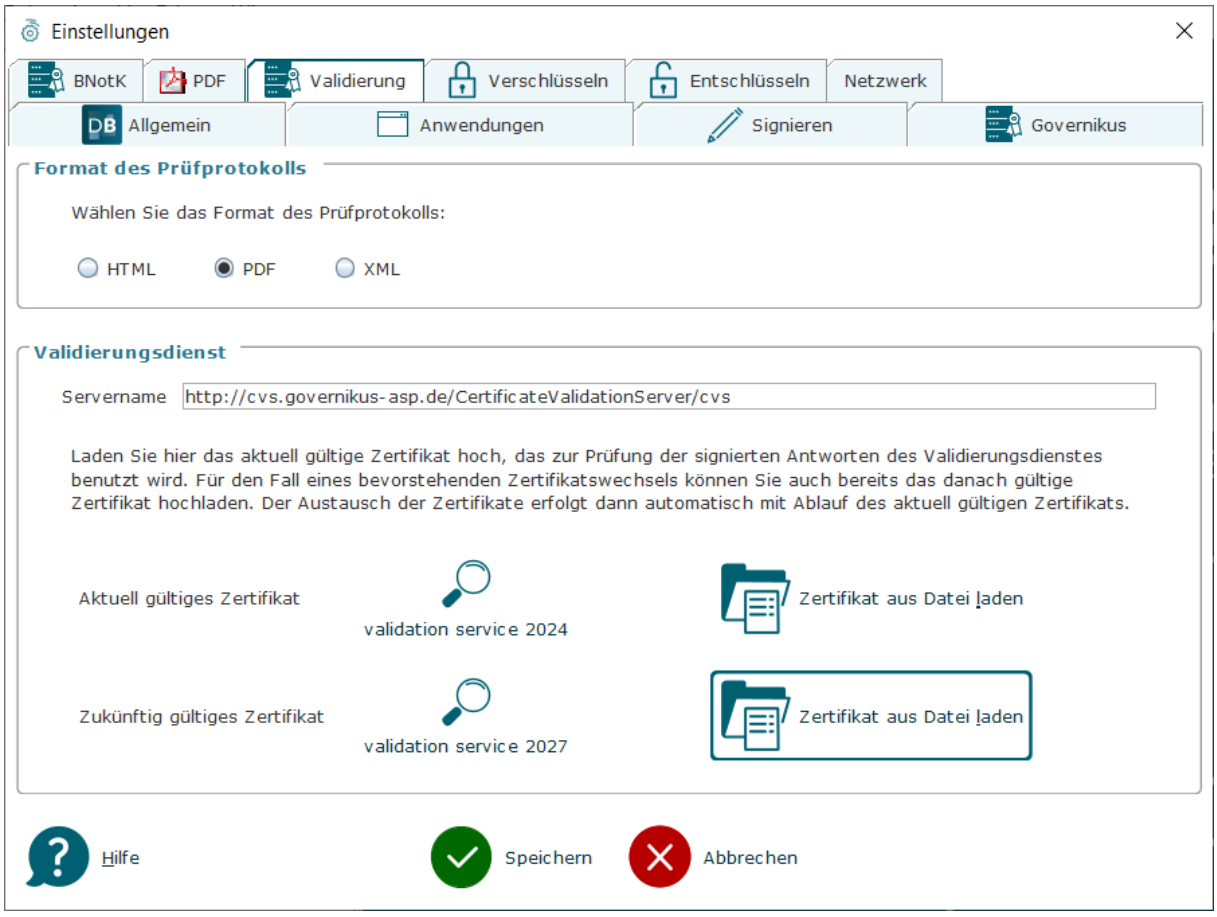

Abbildung 25: Registerkarte Validierung

Tastaturbefehle auf dieser Seite

- Alt + z = Das gewählte Zertifikat wird angezeigt.
- Alt + l = Zertifikat aus Datei laden

5.8 Registerkarte Verschlüsseln

Quelldateien löschen

Sie können hier auswählen, ob nach dem Verschlüsseln die unverschlüsselten Dateien gelöscht werden sollen. Wenn ein Verzeichnis verschlüsselt wurde, wird danach das

unverschlüsselte Quellverzeichnis mit allen Unterverzeichnissen gelöscht. Die Quell-Dateien werden erst nach erfolgreicher Verschlüsselung gelöscht.

Achtung: Die Dateien werden endgültig gelöscht. Es existieren danach nur noch die verschlüsselten Dateien.

Hinweis: Für die Verschlüsselung benutzt DATA Boreum immer die Ciphersuite AES-256-GCM.

Das BSI (siehe technische Richtlinie BSI TR-3116-4) und die IETF (siehe RFC 7525) empfehlen AES-256-GCM für die symmetrische Verschlüsselung und SHA256 als Digest Algorithmus und stufen diese Ciphersuite als sicher ein.

5.9 Registerkarte Entschlüsseln

Quelldateien löschen

Hier können Sie auswählen, ob die verschlüsselten Dateien nach dem Entschlüsseln gelöscht werden sollen. Dies gilt auch für entschlüsselte ZIP-Archive. Die verschlüsselten Dateien werden erst nach erfolgreicher Entschlüsselung gelöscht. **Hinweis**: Die Dateien werden endgültig gelöscht. Es existieren danach nur noch die entschlüsselten Dateien.

5.10 Registerkarte Netzwerk

Wenn ein Proxy-Server zwischen Ihrem Computer und dem Internet steht, müssen Sie hier die Zugangsdaten angeben. Auf dieser Registerkarte sind drei verschiedene Wege vorhanden, einen Proxy-Server zu konfigurieren. Es darf allerdings nur eine Variante genutzt werden. Fragen Sie Ihren Administrator, welche Variante für die Konfiguration eines Proxy-Servers hier genutzt werden soll. Wird DATA Boreum privat genutzt, ist in den meisten Fällen keine Proxy-Konfiguration erforderlich.

Proxy eintragen

Wählen Sie diesen Dialogabschnitt, wenn Sie die Proxy-Serverdaten von Hand eintragen wollen. Sie erhalten die Daten für die Konfiguration des Proxy-Servers von Ihrem Administrator:

- **Servername**: Geben Sie hier den Namen oder die IP-Adresse des Proxy-Servers an, beispielsweise `www.example.com` oder `192.0.32.10`.
- **Port**: Geben Sie hier die Nummer des Ports an, über den die Kommunikation mit dem Proxy-Server durchgeführt wird.
- **Login/Passwort**: Je nach Einstellung des Proxy-Servers kann eine Authentifizierung verlangt werden. Geben Sie in diesem Fall hier Login und Passwort an. Bitte beachten Sie, dass zwischen Groß- und Kleinschreibung unterschieden wird.
- **Ausnahmen**: Sie können hier Ausnahmen eintragen. Eine Ausnahme ist die Adresse eines Computers, der im selben Netzwerk steht, wie Ihr Computer und daher nicht über

den hier angegebenen Proxy-Server zu erreichen ist. Fragen Sie Ihren Administrator, welche Ausnahmen hier eingetragen werden müssen.

PAC eintragen

Wählen Sie diesen Dialogabschnitt, wenn die Proxy-Daten über eine PAC-Datei geladen werden soll. Eine Proxy-Auto-Configuration-Datei (PAC) enthält alle in einem Bereich, beispielsweise in einer Abteilung oder Firma, vorhandenen Proxy-Einstellungen. PAC-Dateien werden üblicherweise von einem Administrator erstellt und verwaltet und liegen auf einem von allen erreichbaren Server.

- **PAC-Datei**: Geben Sie in diesem Feld die Adresse und den Namen der PAC-Datei an. Diesen Pfad erhalten Sie von ihrem Administrator. Beispiel (Windows):
  - `\\example\proxy-settings\abteilung-01.pac`

Proxy-Systemeinstellungen laden

Wählen Sie diesen Dialogabschnitt, wenn Sie die Proxy-Daten über die Systemeinstellungen Ihres Computers laden wollen.

- **Proxy-Systemeinstellungen laden**: Mit dem Button unter diesem Dialogabschnitt können Sie die Proxy-Konfiguration laden, die in den Systemeinstellungen hinterlegt ist. Es handelt sich um die Proxy-Einstellungen, die auf ihrem Computer hinterlegt sind.

Mit dem Speichern wird die Proxy-Konfiguration wirksam. Die folgende Abbildung zeigt die Konfiguration eines Proxy-Servers mit Beispieldaten.

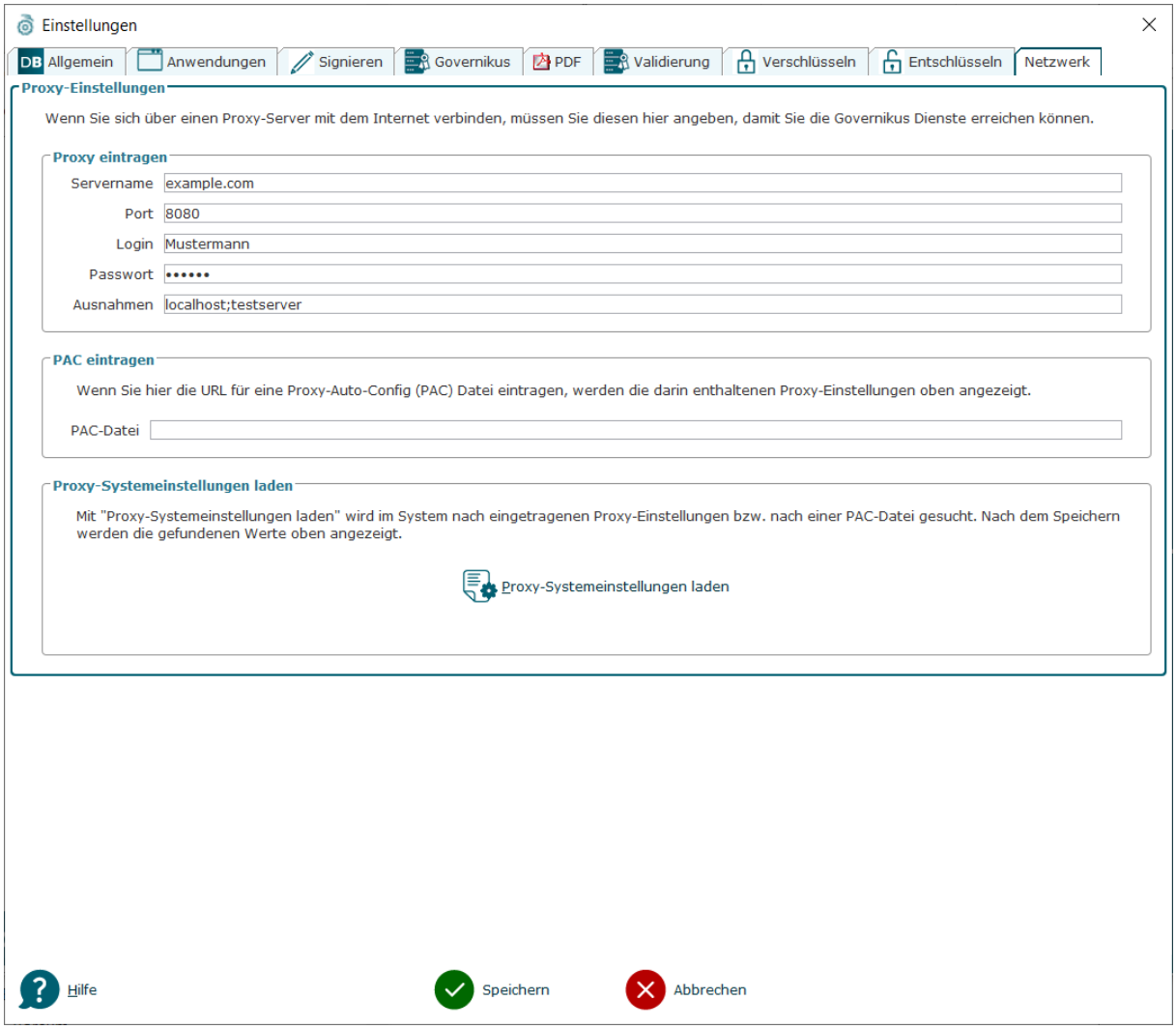

Abbildung 26: Registerkarte Netzwerk mit Beispieldaten

5.11 Einstellungen exportieren

Alle Konfigurationen, die Sie auf den Registerkarten des Dialogs Einstellungen vorgenommen haben, werden in der Datei `data_boreum.xml` gespeichert, die Sie hier finden:

- Windows: `C:\<Profil-Pfad>\<login-name>`
- Linux: `/home/<login-name>`

Dabei steht `<login-name>` für den Namen Ihres Profils auf dem Rechner.

Administratoren können diese Datei exportieren und beispielsweise auf einem Server ablegen, der firmenweit erreichbar ist. Mit der im Kapitel 6.1 erklärten Option "Einstellungen importieren" kann diese Datei importiert werden. Damit können alle Governikus DATA Boreum-Arbeitsplätze mit denselben Einstellungen betrieben werden. Bitte beachten Sie dabei diese Hinweise zu den einzelnen Registerkarten des Einstellungen-Dialogs:

- **Registerkarte Allgemein**: Beachten Sie beim Protokollverzeichnis, dass das Laufwerk auf den Zielrechnern existieren muss.
- **Registerkarte Anwendungen**: Beachten Sie bei Anwendungen, dass diese auf dem Zielrechner unter dem gleichen Pfad abgelegt sein müssen.

- **Registerkarte Validierung**: Alle Angaben werden direkt übernommen. Es wird auch das Zertifikat exportiert.
- **Registerkarte Netzwerk**: Alle Angaben werden direkt übernommen.

	**Hinweis**: Die Optionen zum Importieren und exportieren der Einstellungen finden Sie auch im Kapitel 6.1, in dem die Menüleiste von Governikus DATA Boreum erklärt wird.

6 Hauptfunktionen von Governikus DATA Boreum

Governikus DATA Boreum hat vier Hauptfunktionen. Sie erreichen die benötigte Funktion durch Anklicken des entsprechenden Symbols.

-  **Signieren**: Bietet das elektronische Signieren einer oder mehrerer Dateien.
-  **Validieren**: Ermöglicht den Nachweis von Integrität und Authentizität von elektronisch signierten Dateien.
-  **Verschlüsseln**: Wandelt eine oder mehrere Dateien in eine geheime Repräsentation um.
-  **Entschlüsseln**: Wandelt eine oder mehrere Dateien aus der geheimen Repräsentation in die originale Repräsentation zurück.

6.1 Menüleiste von Governikus DATA Boreum

Die Menüleiste bietet die Menüs "Datei", "Extras" und "Hilfe".

Menü Datei

Das Menü Datei bietet die Funktionen Signieren, Validieren, Verschlüsseln, Entschlüsseln und Beenden. "Beenden" schließt das Fenster und beendet Governikus DATA Boreum. Die anderen vier Funktionen sind nachfolgend in eigenen Kapiteln erklärt.

Menü Ansicht

Das Menü Ansicht bietet diese Funktionen:

- **Sprache**: Sie können Governikus DATA Boreum in Deutsch oder Englisch benutzen. Die Umschaltung wirkt sich sofort aus und kann jederzeit wieder umgestellt werden.
- **Schriftgröße**: In dieser Option können Sie die Schriftgröße zwischen klein, normal und groß umschalten. Bitte beachten Sie, dass nur die Schriftgröße verändert wird, die Größe des Dialogfensters und die Größe von Bildern bleiben gleich.
- **Ausgeblendete Dialoge reaktivieren**: Bestimmte Dialogfenster bieten über eine Checkbox die Option "Diesen Dialog nicht mehr anzeigen". Wenn Sie die Option "Ausgeblendete Dialoge reaktivieren" auswählen, werden wieder alle Dialoge angezeigt, deren Anzeige Sie zuvor unterdrückt haben.

Menü Extras

Das Menü Extras bietet diese Funktionen:

- **Einstellungen**: Diese Option ruft den Dialog "Einstellungen" auf, der in Kapitel 5 erklärt ist.
- **Einstellungen importieren**: Mit dieser Option können Sie eine Datei importieren, die bereits Einstellungen für Governikus DATA Boreum enthält. So ist es beispielsweise möglich, firmenweit dieselben Einstellungen zu verwenden. **Achtung**: Sollten Sie bereits eigene Einstellungen vorgenommen haben, werden diese durch diesen Import

überschrieben. Die Bereitstellung einer Datei mit vorkonfigurierten Einstellungen ist im Kapitel 5.11 beschrieben.

- **Einstellungen exportieren**: Wenn Sie diese Option wählen, können Sie über einen Dateiauswahldialog die Einstellungen von Governikus DATA Boreum in einer Datei abspeichern. Die Datei hat die Endung `.xml`. Welche Einstellungen in dieser Datei enthalten sind, ist in Kapitel 5.11 erklärt.
- **Einstellungen zurücksetzen**: Mit dieser Option werden alle Einstellungen gelöscht. Die Einträge in den Registerkarten des Dialogfensters Einstellungen werden auf die Werkseinstellungen zurückgesetzt.
- **Protokolldatei anzeigen**: Die Protokolldatei ist eine ASCII-Datei mit der Endung `.txt`. Wenn Sie diese Option wählen, wird die Protokolldatei mit dem Anzeigeprogramm aufgerufen, das auf Ihrem Computer mit der Dateiendung `.txt` assoziiert ist. **Hinweis**: Diese Option ist nur benutzbar, wenn Sie auf der Registerkarte "Allgemein" das Protokollieren der Programmaktivitäten ausgewählt haben. Wenn diese Option nicht ausgewählt ist, ist diese Option ausgegraut.
- **Protokolldatei senden**: Diese Option ruft das E-Mail-Programm auf, das auf Ihrem Computer für E-Mails eingerichtet ist. Der Adressat ist entweder der Helpdesk der Governikus KG oder der Dienstanbieter, der Ihnen Governikus DATA Boreum zur Verfügung stellt. Die Protokolldatei ist als Dateianhang bereits hinzugefügt. Im Textteil dieser E-Mail ist ein Formular vorbereitet, das Sie für den Support bitte ausfüllen. **Hinweis**: Diese Option ist nur benutzbar, wenn Sie auf der Registerkarte "Allgemein" das Protokollieren der Programmaktivitäten ausgewählt haben. Wenn diese Option nicht ausgewählt ist, ist diese Option ausgegraut.

Das Menü Hilfe

Das Menü Hilfe bietet diese Funktionen:

- **Hilfe**: Diese Option ruft die Online-Hilfe auf.
- **Lizenz**: Über diesen Menüeintrag erreichen Sie den Dialog zur Eingabe des Lizenzschlüssels. Der Lizenzschlüssel ist in Kapitel 3.6 erklärt.
- **Über Governikus DATA Boreum**: Über diese Option wird ein Dialogfenster angezeigt, das Informationen über die Version und den Hersteller enthält.

	**Hinweis**: Bitte beachten Sie, dass das Menü "Extras" in der Governikus DATA Boreum Integration Edition andere Optionen hat.

Die folgende Abbildung zeigt die Einstiegsseite von Governikus DATA Boreum.

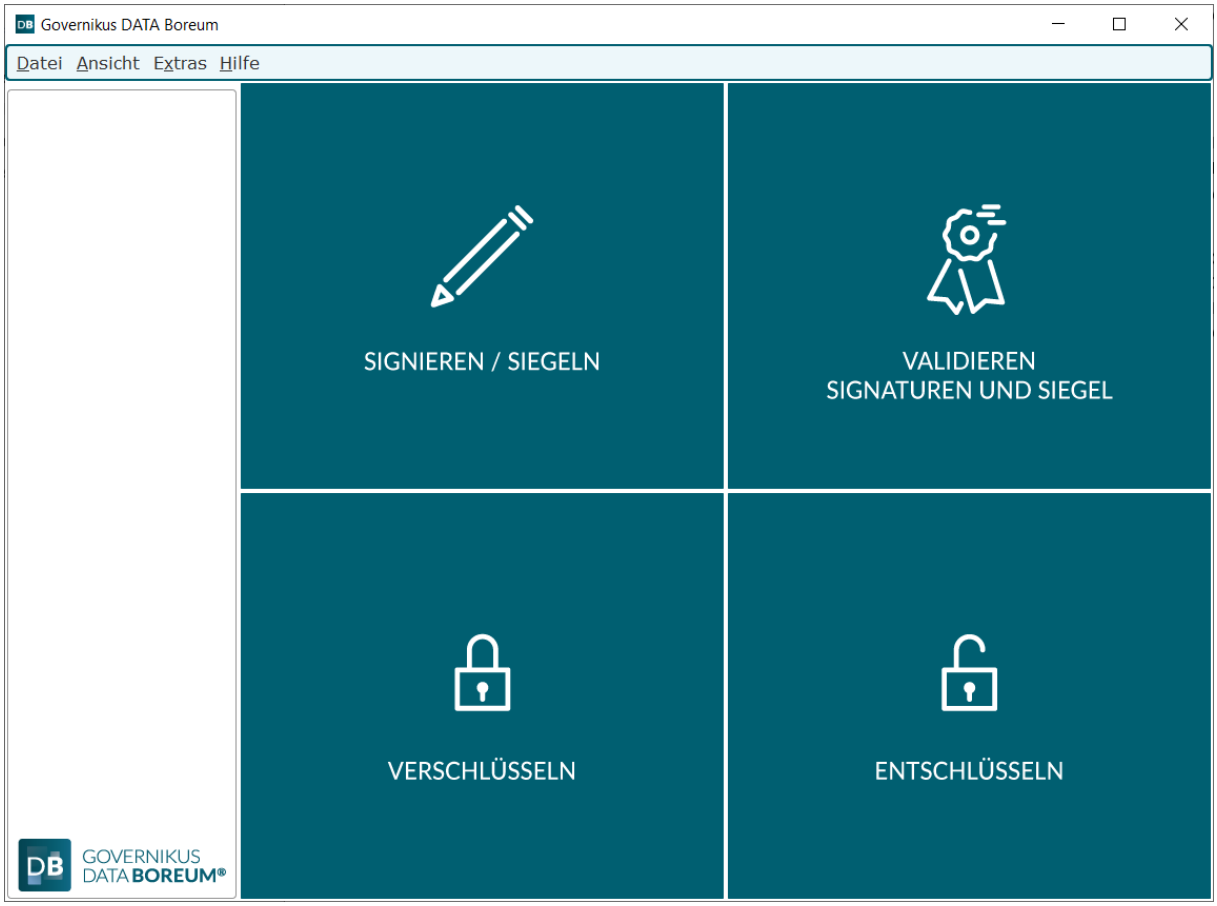

Abbildung 27: Einstiegsseite von Governikus DATA Boreum

6.2 Tastaturbefehle

Der Governikus lässt sich über die Tastatur steuern.

	Hinweis: Neben den Befehlen in den Menüs der Menüleiste stehen die verfügbaren Tastaturbefehle.

Im Folgenden werden die Tastaturbefehle aufgelistet, die die Bedienung von Governikus DATA Boreum über die Tastatur ermöglichen.

Tastaturbefehle der Einstiegsseite

- Strg + 1 = Signieren
- Strg + 2 = Validieren
- Strg + 3 = Verschlüsseln
- Strg + 4 = Entschlüsseln
- Alt + d = Aufruf des Menüs "Datei"
- Alt + x = Aufruf des Menüs "Extras"
- Alt + h = Aufruf des Menüs "Hilfe"

Diese Tastaturkürzel sind bei macOS nicht verfügbar.

Sie können mit der Tabulator-Taste durch die Einstiegsseite navigieren. Wenn Sie die gewünschte Funktion mit dem Tabulator erreicht haben, nutzen Sie die Leertaste, um die Funktion aufzurufen.

Allgemein gültige Tastaturbefehle

- Alt + F4 = Programm beenden
- F1 = Hilfe aufrufen

macOS Benutzer benutzen bitte die entsprechenden Tasturkürzel des Systems.

Tastaturbefehle innerhalb einer ausgewählten Funktion

- Alt + (Pfeil nach unten) = Den nächsten Schritt der Navigation auswählen
- Alt + (Pfeil nach oben) = Den vorherigen Schritt der Navigation auswählen
- Alt + (Pfeil nach rechts) = Den nächsten Schritt der Navigation auswählen (Dialoge, die als "Standardeinstellung" markiert sind, werden dabei übersprungen)
- Enter = Wie "Alt + (Pfeil nach rechts)"
- Alt + (Pfeil nach links) = den vorherigen Schritt der Navigation auswählen (Dialoge, die als "Standardeinstellung" markiert sind, werden dabei übersprungen)
- Alt + Backspace = zurück zur Startseite

Diese Tastaturkürzel sind bei macOS nicht anwendbar.

- F1 = Kontextsensitive Hilfe - macOS Benutzer benutzen bitte das entsprechende Tasturkürzel des Systems.

Tastaturbefehle innerhalb der Zertifikatsansicht

- Strg + s = Zertifikat speichern
- Enter = Fenster schließen
- Esc = Fenster schließen

	**Hinweis**: In einigen Fällen ist ein Verlassen bestimmter Dialogelemente über die Tabulator-Taste nicht möglich, beispielsweise in Tabellenelementen wie der Dateiliste. Diese Tastaturfalle können Sie mit der Kombination Strg + Tab (vorwärts) oder Strg + Shift + Tab (rückwärts) verlassen.

6.3 Gemeinsame Merkmale der Dialogseiten

Nachdem Sie eine Funktion auf der Einstiegsseite ausgewählt haben, wird Ihnen der Funktionsdialog angezeigt, von dem aus Sie durch die Einstellungen bis zur Ausführung der Funktion geführt werden. Der Aufbau der Seiten ist immer gleich.

- **Menü**: Das Menü oben links steht immer zur Verfügung. Die Menüs sind in Kapitel 6.1 erklärt.
- **Linke Seite**: Auf der linken Seite finden Sie eine Buttonleiste zur Dialogseitenauswahl, die Sie nacheinander aufrufen können. Auf der letzten Dialogseite kann dann die

anfangs ausgewählte Funktion mit den zuvor gewählten Einstellungen ausgeführt werden.

- **Rechte Seite, oben**: Rechts auf jeder Dialogseite befindet sich in der Mitte oben eine Überschrift. Diese bezeichnet den jeweiligen Dialogschritt und stimmt mit dem blau gerahmten Button der Dialogseitenauswahl auf der linken Seite überein. Sie soll Ihnen die Orientierung erleichtern.
- **Rechte Seite, Mitte**: In diesem Bereich können Sie Einstellungen vornehmen oder Aktionen auslösen.
- **Rechte Seite, unten**: Hier finden Sie Buttons zur Navigation durch die Dialogseiten, siehe Abschnitt Navigation weiter unten.

Standardeinstellungen

Einige Seiten bieten die Möglichkeit, die gewählte Einstellung zu speichern. Klicken Sie dazu auf die Checkbox "Als Standardeinstellung speichern" unten auf der Seite.

	**Hinweis**: Bitte beachten Sie, dass die Option "Als Standardeinstellung speichern" in der Governikus DATA Boreum Integration Edition nicht verfügbar ist.

6.3.1 Navigation durch die Dialogseiten

- **Dialogseitenauswahl**: Jede Dialogseite kann direkt durch Anklicken der entsprechenden Dialogseitenauswahl auf der linken Seite aufgerufen werden. Die folgende Abbildung zeigt die Dialogseitenauswahl beispielhaft für die Funktion Signieren. Dabei ist die gerade ausgewählte Dialogseite blau umrandet. Wenn auf einer Dialogseite noch Einstellungen ausgewählt werden müssen, ist der nummerierte Kreis weiß, sonst ist er blau.

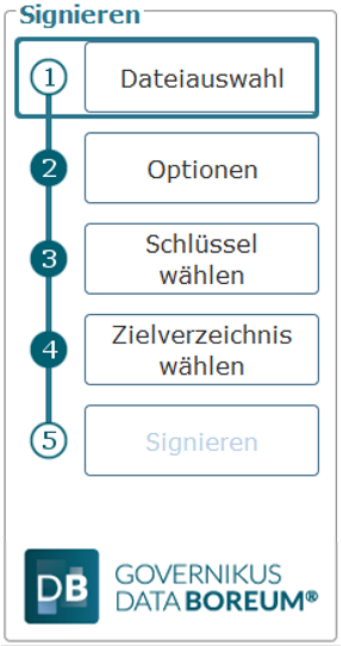

Abbildung 28: Dialogseitenauswahl am Beispiel Signieren

-  : Rufen Sie über diesen Button die Hilfe auf.
-  **Schriftgröße**: Die Buchstaben "a" können einzeln angeklickt werden um die Schriftgröße zwischen kleiner (Voreinstellung), normal und größer zu ändern.
-  : Unten rechts finden Sie Vor- und Zurück-Pfeile. Mit diesen Pfeilen können Sie zwischen den Dialogseiten hin- und herschalten. Dabei werden die Seiten übersprungen, auf denen Sie die Checkbox "Als Standardeinstellung speichern" ausgewählt haben (siehe oben). Sollten auf einer Dialogseite erforderliche Eingaben fehlen, ist der Vor-Pfeil nicht auswählbar.
-  : Dieser nach links unten zeigende Pfeil befindet sich jeweils auf der letzten Dialogseite einer Funktion und führt Sie direkt zurück auf die erste Seite (Dateiauswahl) dieser Funktion. Dabei bleiben die Dateien, die nicht verarbeitet wurden, in der Dateiauswahl erhalten. Die erfolgreich verarbeiteten Dateien werden nicht mehr aufgelistet.
-  : Auf jeder Dialogseite können Sie mit dem Abbrechen-Button zur Einstiegsseite von Governikus DATA Boreum zurückkehren.
-  : Nach Abschluss eines Vorgangs wird anstelle des Abbrechen-Buttons (siehe oben) dieser OK-Button angezeigt, über den Sie ebenfalls zur Einstiegsseite zurückkehren können.

	**Hinweis**: Alle Buttons, auch wenn ausgegraut, haben Tooltips. Buttons werden ausgegraut, wenn benötigte Einstellungen fehlen. Ist ein Funktionsbutton der jeweils letzten Dialogseite ausgegraut, gibt hier der Tooltip die Ursache an.

6.3.2 Dateiauswahl

Der Dialog Dateiauswahl ist für alle Funktionen gleich. Auf der rechten Seite finden Sie eine Liste, die anfangs leer ist. Sie können beliebig viele Dateien aus verschiedenen Verzeichnissen auswählen. Sie können der Liste auf drei 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 von Governikus DATA Boreum.

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.

3. Übergabe per Kontextmenü

Hinweis: Für macOS Benutzer steht das Kontextmenü nicht zur Verfügung.

Sie können im Dateimanager eine oder mehrere Dateien markieren und durch einen Rechtsklick das Kontextmenü aufrufen. Sollten im Dialogfenster "Dateiauswahl" von Governikus DATA Boreum bereits Dateien enthalten sein, werden Sie in einem

Extradialogfenster gefragt, ob Sie die vorhandene Auswahl ersetzen, oder die ausgewählten Dateien hinzufügen wollen.

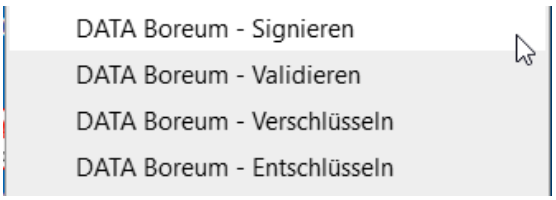

Abbildung 29: DATA Boreum Kontextmenü im Windows Explorer

Wenn Sie über das Kontextmenü einen bestimmten Boreum Prozess auswählen, beispielsweise Signieren, und in Governikus DATA Boreum ist bereits ein anderer Prozess geöffnet, beispielsweise Validieren, werden Sie gefragt, ob Sie diesen verlassen wollen, siehe nächste Abbildung.

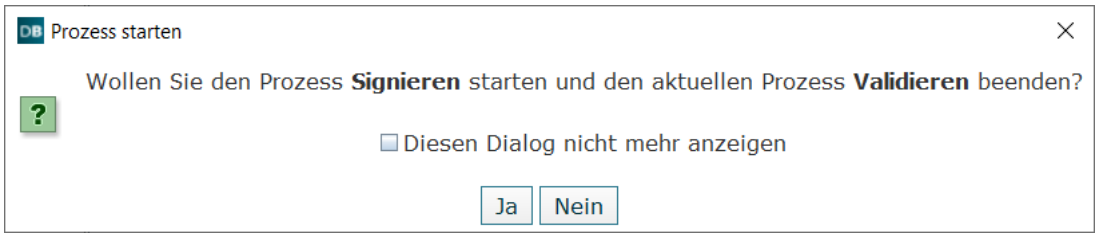

Abbildung 30: Hinweisdialog zum Prozesswechsel

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 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 Governikus DATA Boreum 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 (siehe auch Kapitel 5.1, Abschnitt Mindestanzahl). 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.

6.3.3 Zielverzeichnis wählen

Auch die Dialogseite "Zielverzeichnis wählen" existiert für jede Funktion von Governikus DATA Boreum. Bei der Funktion "Validieren" ist diese Auswahl auf der Dialogseite "Einstellungen" zu finden, sonst unter dem angegebenen Namen.

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.

Sie haben in diesem Dialog die Möglichkeit, Ihre Auswahl zu speichern. Benutzen Sie dazu die Checkbox "Als Standardeinstellung speichern und nicht mehr fragen." am unteren Rand der Dialogseite. Die nächste Abbildung zeigt den Dialog, bei dem die Auswahl "Quellverzeichnis nutzen" ausgewählt ist.

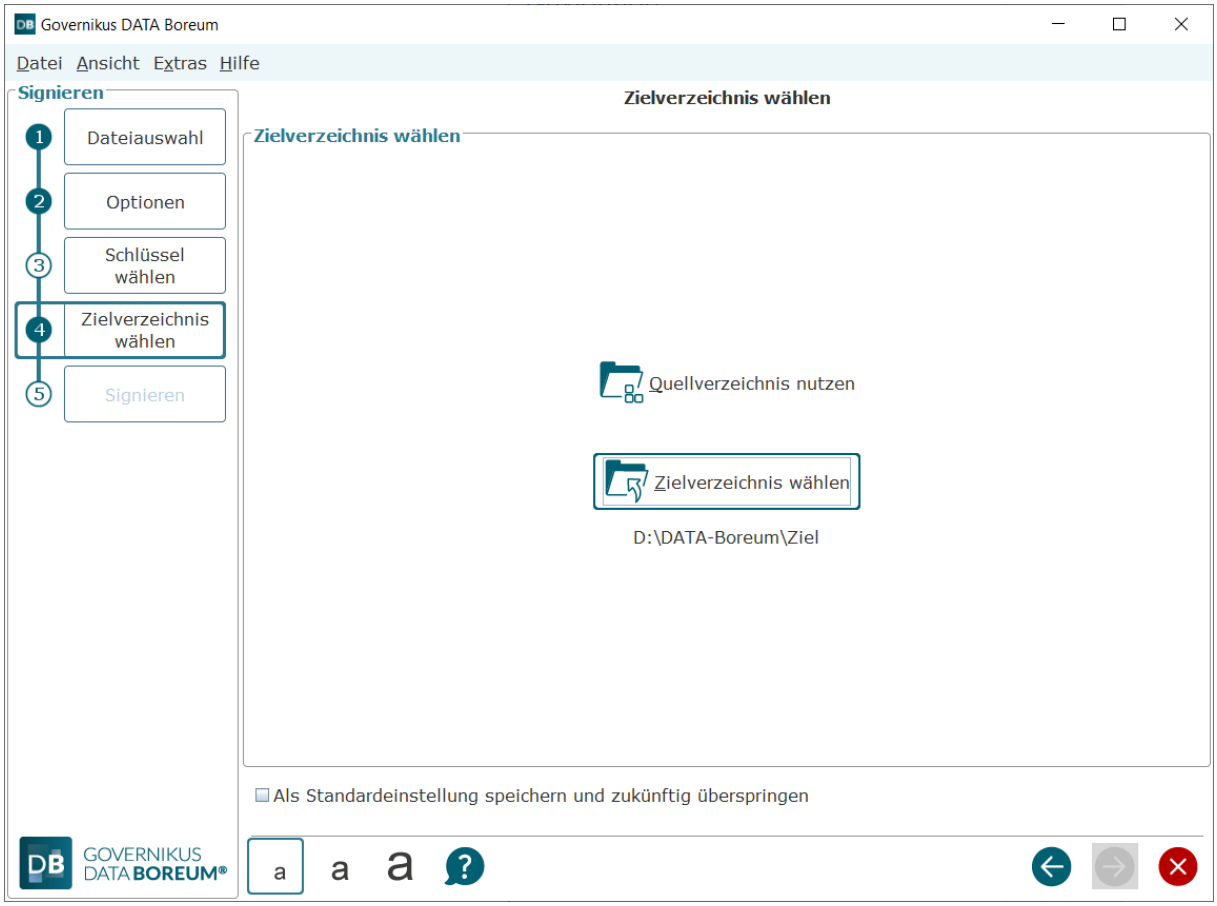

Abbildung 31: Dialogseite Zielverzeichnis wählen

6.4 Signieren

In diesem Dialog können Sie Dateien elektronisch signieren. Eine Erklärung zur elektronischen Signatur finden Sie im Anhang "Erläuterungen" im Kapitel 9.3.

Aufruf

Klicken Sie auf der Einstiegsseite von Governikus DATA Boreum auf "Signieren", benutzen Sie alternativ das Tastaturkürzel "Strg + 1".

Aufruf mit Datei

Hinweis: Für macOS Benutzer steht das Kontextmenü nicht zur Verfügung.

Sie können im Dateimanager Dateien auswählen und aus dem Kontextmenü "Signieren" wählen. Sollte Governikus DATA Boreum noch nicht gestartet sein, so wird er mit Ihrer Auswahl gestartet. Sollte Governikus DATA Boreum bereits gestartet sein und Sie wählen eine Datei über das Kontextmenü, so ersetzt die ausgewählte Datei alle Dateien, die möglicherweise bereits zuvor ausgewählt waren. Die folgende Abbildung zeigt das Kontextmenü.

6.4.1 Dateiauswahl

Wählen Sie hier die Dateien aus, die Sie elektronisch signieren wollen. Die Dateiauswahl ist in Kapitel 6.3.2 erklärt.

Die Dateiliste

Die Dateiliste zeigt zeilenweise die von Ihnen zum Signieren ausgewählten Dateien. Dabei haben die Spalten diese Bedeutung:

- **Datei**: Zeigt den Dateinamen an. Wenn Sie den Mauszeiger über den Dateinamen legen, wird der vollständige Pfad angezeigt.
-  : Dieses Symbol wird angezeigt, wenn die Datei vor dem Signieren angezeigt wurde (siehe auch Kapitel 5.3, Abschnitt Mindestanzahl). Das Symbol ist grau, wenn die Datei noch nicht angezeigt wurde.
- **Dateiendungen**: Über Dateiendungen 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`.

Tastaturbefehle auf dieser Seite

- Alt + a = Datei hinzufügen
- Entf = Ausgewählte Dateien entfernen
- Alt + t = Fokus in die Tabelle setzen
- Alt + P = Dialogseite zum Erstellen von Signaturfeldern aufrufen

6.4.2 Sonderfall PDF-Datei

Wenn Sie in einer PDF-Datei mehrere sichtbare Signaturen anbringen wollen, können Sie die PDF-Datei mit Governikus DATA Boreum vorbereiten. Dies kann beispielsweise in einem Szenario notwendig sein, in dem sichtbare Signaturen von mehreren Personen erforderlich sind. Wenn Sie eine PDF-Datei in die Dateiauswahl aufnehmen, können Sie mit einem Rechtsklick auf die PDF-Datei das Kontextmenü "Signaturfelder anlegen" aufrufen. Dieser Aufruf über das Kontextmenü ist auf der Dialogseite "Dateiauswahl" und auf der Dialogseite "Signieren" möglich. Die nächste Abbildung zeigt das Kontextmenü.

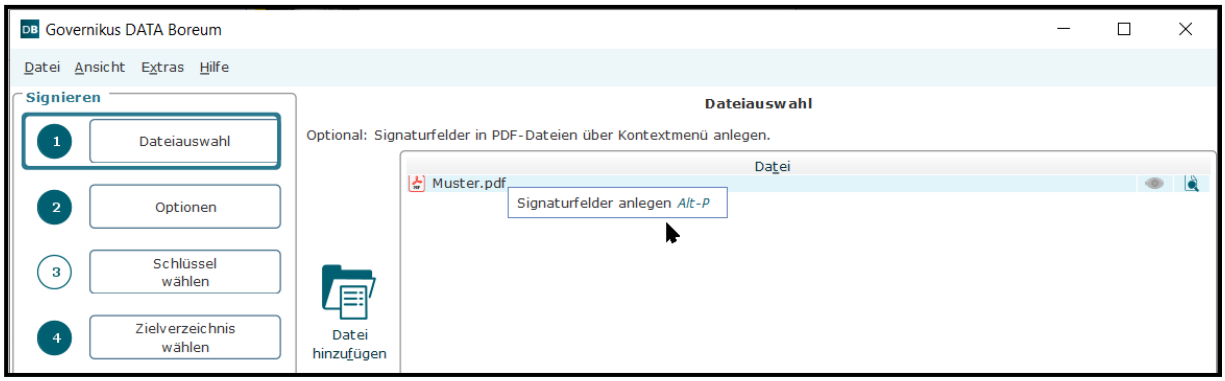

Abbildung 32: Kontextmenü in der Dateiauswahl

Dieses Kontextmenü ruft ein neues Dialogfenster auf, in dem Sie in der ausgewählten PDF-Datei leere Signaturfelder einfügen können. In diese Felder werden beim Signieren sichtbare Elemente eingefügt.

Achtung: Wenn Sie diese Funktion benutzen, wird die PDF-Datei mit den sichtbaren Signaturfeldern im Quellverzeichnis verändert und gespeichert.

Dialogseite "Erweiterte PDF-Signatur"

Auf dieser Dialogseite können Sie Felder anlegen, die sichtbare Signaturen in PDF-Dokumenten aufnehmen können.

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

- Auf der Dialogseite "Dateiauswahl" über das Kontextmenü, in diesem Kapitel beschrieben
- Auf der Dialogseite "Signieren" über das Kontextmenu in der Dateiliste, siehe Kapitel 6.4.6.
- Beim Auslösen des Signiervorgangs, wenn die Dialogseite angezeigt wird, siehe Kapitel 6.4.6.

Mitte der Dialogseite

In der Mitte der Dialogseite wird der Inhalt der PDF-Datei angezeigt. Unter dieser Anzeige ist 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.

Die folgende Abbildung zeigt den Dialog zum Anlegen von Signaturfeldern mit einem Beispiel.

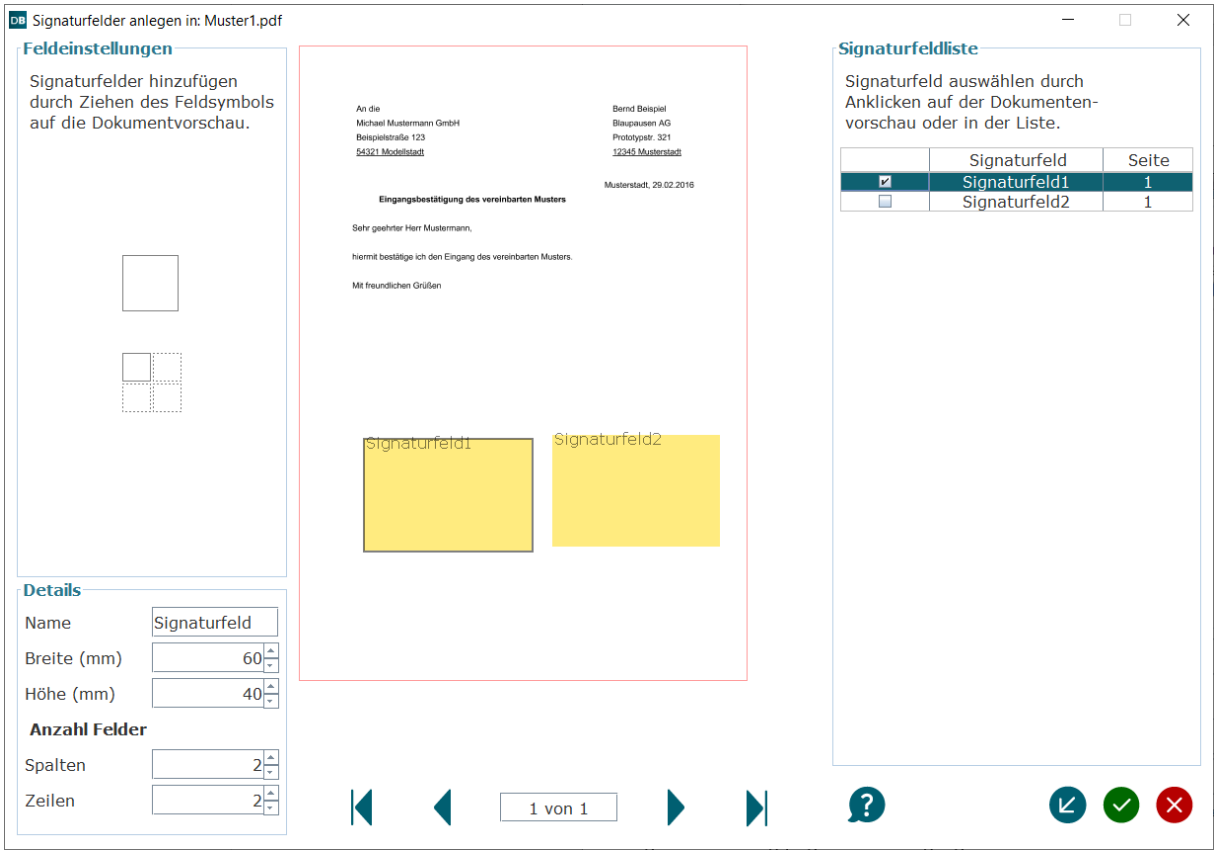

Abbildung 33: Dialogseite zum Anlegen von Signaturfeldern

6.4.3 Optionen für die Funktion Signieren

Auf der Dialogseite Optionen können Sie das Signaturformat auswählen und weitere Signaturkonfigurationen vornehmen. Vergewissern Sie sich bei der Auswahl des Signaturformats, dass dieses Format vom Empfänger zugelassen und akzeptiert ist. Governikus DATA Boreum unterstützt verschiedene, international standardisierte Formate für elektronische Signaturen. Diese unterstützten Formate sind im Anhang "Erläuterungen" im Kapitel "9.4" erklärt.

6.4.3.1 Standardsignaturformat wählen (CAdES)

- **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`.
- **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" von Governikus DATA Boreum 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.

6.4.3.2 Signieren von PDF-Dokumenten (PAdES)

In diesem Dialogabschnitt wählen Sie zuerst, in welchem Format die PDF-Datei signiert werden soll.

- Das Standardsignaturformat (CAdES) wird für PDF-Dateien eher selten gewählt.
- Das PAdES-Format ist das übliche Format für das Signieren von PDF-Dateien.

Auswahl des Signaturformats

- **Standardsignaturformat verwenden**: PDF-Dateien werden, wie alle anderen Dateien, in dem Format signiert, das unter **Standardsignaturformat (CAdES)** ausgewählt ist, siehe Abschnitt oben. Diese Einstellung wird für PDF-Dateien eher selten genutzt.

Mit der folgenden Option legen Sie fest, dass Sie das für PDF-Dateien typische PAdES-Signaturformat nutzen wollen.

Achtung: Bitte beachten Sie unbedingt, dass die Einstellungen für die PDF-Signatur weitestgehend durch die Konfiguration auf der Registerkarte „PDF“ in den „Einstellungen“ bestimmt wird und nicht über diesen Dialogabschnitt! Lesen Sie dazu Kapitel 5.6.

- **PDF-Signatur erstellen**: Wenn Sie diese Option wählen, erreichen Sie die sonst ausgegrauten Felder „Signaturfeld-Vorlage“, „Grund der Unterschrift“ und „Ort“. Bei diesem Format wird die Signatur innerhalb der PDF-Datei abgelegt. Eine so signierte PDF-Datei hat die Endung `_signed.pdf`.
  - **Signaturfeld-Vorlage**: Wenn Sie bereits Vorlagen erstellt oder importiert haben, können Sie hier eine Vorlage auswählen. Wenn Sie die Option "Keine" wählen, wird die PDF-Signatur mit den Einstellungen vorgenommen, die im Dialogfenster "Einstellungen" in der Registerkarte "PDF" gespeichert sind. Sie erreichen die Registerkarte "PDF" über den Link "Signatureinstellungen" rechts über der Auswahlliste. Die Registerkarte "PDF" ist im Kapitel 5.5 erklärt.
  - **Grund der Unterschrift**: Hier können Sie den Grund Ihrer Unterzeichnung (z. B. "sachlich richtig" oder "zur Zahlung freigegeben") eintragen. Es können maximal 50 Zeichen eingegeben werden. Wenn Sie keinen Grund angeben möchten, lassen Sie dieses Eingabefeld einfach leer.
  - **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.

6.4.3.3 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.

6.4.3.4 Zeitstempel

Wenn Sie in den Einstellungen auf der Registerkarte „Governikus“ den Authentisierungsdienst und den Zeitstempeldienst konfiguriert haben, siehe Kapitel 5.4, 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 7.1.

Standardeinstellung

Wie im Kapitel 6.3 erklärt, können Sie die auf dieser Dialogseite vorgenommen Einstellungen als Standardeinstellungen speichern. Wenn Sie zukünftig beim Signieren über die blauen Navigationspfeile rechts unten navigieren, wird diese Seite nicht mehr angezeigt.

6.4.4 Schlüssel wählen

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

6.4.4.1 Signaturniveau

In diesem Dialogabschnitt können Sie vorgeben, mit welchem Signaturniveau Sie die Dateien signieren wollen.

Hinweis: Das ausgewählte Signaturniveau wird auf der letzten Dialogseite "Signieren" erneut angezeigt. Bitte überprüfen Sie auf dieser Seite erneut die gewählte Einstellung.

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.

- **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.
- **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 Chipkartenleser 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.

6.4.4.2 Speicherort des Schlüssels

In diesem Dialogabschnitt können Sie auswählen, woher Sie den Schlüssel für die Erstellung der Signatur beziehen wollen. Die folgenden Kapitel erklären die Möglichkeiten in diesem Dialogabschnitt.

6.4.4.2.1 Schlüssel aus Datei laden

Bitte beachten Sie, dass Sie mit einem Schlüssel aus einer Datei **nur fortgeschrittene Signaturen** erstellen können. Sie müssen daher im Dialogabschnitt „Signaturniveau“, siehe oben, die Option „Fortgeschritten“ auswählen. Wenn das Signaturniveau „Qualifiziert“ ausgewählt ist, ist die Option „Schlüssel aus Datei laden“ ausgegraut.

Wenn Sie einen Schlüssel aus einer Datei laden wollen, klicken Sie auf das Symbol „Schlüssel aus Datei laden“ 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. Lesen Sie dazu auch das Kapitel 9.8 über 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 Identifikationsunterlagen vorgelegt haben. Beim Laden der Keystore-Datei werden Sie nach der PIN für den Keystore gefragt. Beachten Sie die Reihenfolge:

- **Signaturniveau festlegen**: Stellen Sie das Signaturniveau auf „Fortgeschritten“ ein.
- **Schlüssel aus Datei laden**: Wählen Sie einen Keystore aus und geben Sie die PIN ein.
- **Schlüssel auswählen**: Wenn ein oder mehrere Schlüssel im Keystore gefunden werden, die zum Erstellen einer Signatur geeignet sind, werden diese hier angezeigt. Enthält der Keystore keine Schlüssel, die zum Signieren geeignet sind, wird eine Fehlermeldung angezeigt. Wählen Sie durch Anklicken den Schlüssel aus, den Sie zum Signieren verwenden wollen.

Die folgende Abbildung zeigt den Auswahldialog mit einem Beispiel-Keystore.

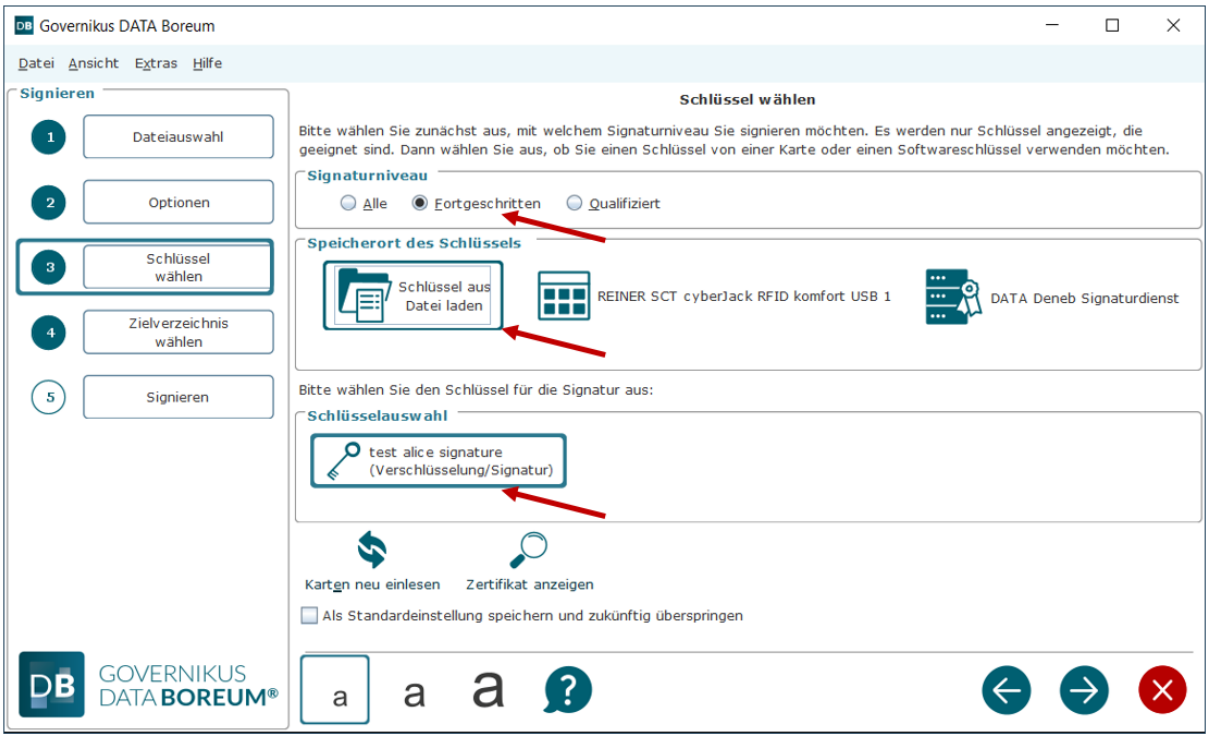

Abbildung 34: Auswahl „Schlüssel aus Datei laden“

Merkmale für die Schlüsselauswahl aus einer Datei

- **Signaturniveau**: Beim Signieren mit einem Schlüssel aus einer Datei ist das Signaturniveau „Fortgeschritten“. Im Dialogabschnitt „Signaturniveau“, siehe Kapitel 6.4.4.1, muss „Fortgeschritten“ ausgewählt sein, da sonst der Button zur Auswahl eines Schlüssels aus einer Datei ausgegraut ist.
- **Beschränkungen**: Sie können eine Datei oder einen Stapel von Dateien zum Signieren mit einem Schlüssel aus einer Datei übergeben. Ein Stapel darf nicht mehr als **500** Dateien umfassen. Die PIN für den Schlüssel aus einer Datei muss nur einmal beim Auswählen der Schlüsselspeicherdatei angegeben werden. Danach können mit diesem Schlüssel, ohne weitere PIN-Eingabe, beliebig viele Dateien signiert werden.
- **Dauer der Schlüsselauswahl**: Der Schlüssel aus einer Datei bleibt als ausgewählter Schlüssel solange wirksam, bis entweder ein anderer Schlüssel ausgewählt wurde, oder DATA Boreum neu gestartet wurde.

6.4.4.2.2 Signaturkarte

Diese Auswahl wird nur angezeigt, wenn Sie einen Chipkartenleser angeschlossen **und** eine Signaturkarte eingesteckt haben. Neben dem Symbol steht der Name des Chipkartenlesers, der von Governikus DATA Boreum erkannt wurde. Sie können bis zu 10 Chipkartenleser anschließen. Zu Chipkartenlesern lesen Sie bitte die mitgelieferten Dokumente zu den Systemvoraussetzungen. Mit einer Signaturkarte können Sie in der Regel qualifizierte elektronische Signaturen erstellen. Beachten Sie die Reihenfolge:

- **Signaturniveau festlegen**: Mit Signaturkarten sollen üblicherweise qualifizierte elektronische Signaturen erstellt werden. Häufig sind auch noch Schlüssel für fortgeschrittene Signaturen auf der Signaturkarte vorhanden. Bitte beachten Sie daher, dass Sie das Signaturniveau auf „Qualifiziert“ einstellen, wenn Sie qualifizierte

elektronische Signaturen erstellen wollen. Nur so werden Ihnen nur die Schlüssel angezeigt, die für qualifizierte elektronische Signaturen geeignet sind.

- **Chipkartenleser verbunden und Signaturkarte eingesteckt**: Die Schlüsselauswahl für die Signaturkarte wird nur angezeigt, wenn ein Chipkartenleser verbunden und Signaturkarte eingesteckt ist.
- **Schlüssel auswählen**: Es werden die Schlüssel auf der Signaturkarte angezeigt, die zum Erstellen einer qualifizierten elektronischen Signatur geeignet sind. Wählen Sie durch Anklicken den Schlüssel aus, den Sie zum Signieren verwenden wollen.

Die folgende Abbildung zeigt den Auswahldialog mit einem Beispiel.

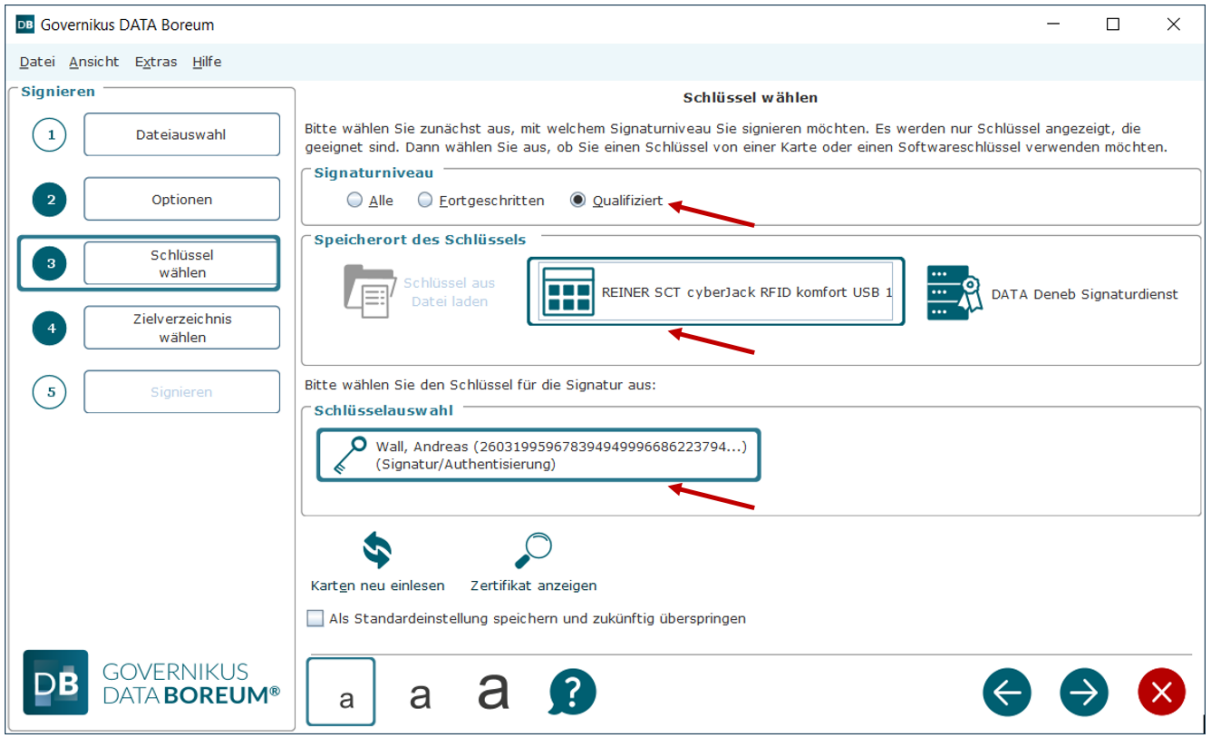

Abbildung 35: Auswahl „Schlüssel von Signaturkarte“

Merkmale für die Schlüsselauswahl von einer Signaturkartei

- **Signaturniveau**: Das Signaturniveau ist abhängig von der Festlegung des Signaturniveaus im Dialogabschnitt über der Schlüsselauswahl, siehe Kapitel 6.4.4.1.
  - Wenn Sie das Signaturniveau „Fortgeschritten“ ausgewählt haben, werden Ihnen alle Signaturzertifikate für fortgeschrittene und qualifizierte elektronische Signaturen angezeigt, die auf der Signaturkarte gespeichert und gültig sind.
  - Wenn Sie das Signaturniveau „Qualifiziert“ ausgewählt haben, werden Ihnen nur die Signaturzertifikate für qualifizierte elektronische Signaturen angezeigt, die auf der Signaturkarte gespeichert und gültig sind.
- **Beschränkungen**: Sie können eine Datei oder einen Stapel von Dateien zum Signieren mit der Signaturkarte übergeben. Ein Stapel darf nicht mehr als **500** Dateien umfassen.
  - Wenn Sie eine Signaturkarte für Einzelsignaturen nutzen, müssen Sie die PIN für jede Datei angeben, die signiert werden soll.
  - Wenn Sie eine Multisignaturkarte nutzen, müssen Sie die PIN nur einmal pro übergebenen Stapel angeben.

- **Dauer der Schlüsselauswahl**: Die Signaturkarte bleibt als ausgewählter Schlüssel solange wirksam, bis entweder ein anderer Schlüssel ausgewählt wurde, oder DATA Boreum neu gestartet wurde.

Wichtiger Hinweis

Achtung:

- **Chipkartenleser vom Rechner trennen**: Trennen Sie **niemals** einen Chipkartenleser vom Rechner, solange das Programm ausgeführt wird. Beenden Sie das Programm, bevor Sie einen Chipkartenleser vom Rechner trennen.
- **Entfernen der Signaturkarte**: Entfernen Sie **niemals** während des Signaturvorgangs die Signaturkarte aus dem Chipkartenleser. 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 Chipkartenleser verwenden, müssen Sie hier vor der Schlüsselauswahl zunächst die Zugangsnummer eingeben. Die sechsstellige Zugangsnummer ist 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 von Governikus DATA Boreum von der Signaturanwendungskomponente eines anderen Herstellers verwendet, kann es passieren, dass Governikus DATA Boreum die Signaturkarte nicht mehr lesen kann, weil die andere Signaturanwendungskomponente diese nicht freigibt.

Wenn Sie die Signaturkarte wieder mit Governikus DATA Boreum benutzen wollen, verfahren Sie wie folgt:

- Beenden Sie unbedingt die Signaturanwendungskomponente des anderen Herstellers.
- Nehmen Sie die Signaturkarte aus dem Chipkartenleser und stecken Sie sie gleich wieder in den Chipkartenleser 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 Chipkartenleser, in dem die Signaturkarte steckt, ist von dieser Aktion nicht betroffen und arbeitet weiter wie zuvor.

Hinweis: Wenn Sie in den „Einstellungen“ in der Registerkarte „BNotK“ die Option „Ja, der Fernsignaturdienst soll verwendet werden.“ ausgewählt haben, wird die Möglichkeit mit einer Signaturkarte zu signieren in „Speicherort des Schlüssels“ nicht angezeigt.

6.4.4.2.3 Signieren mit dem Signaturdienst

Wenn der Signaturdienst konfiguriert wurde, kann hier auch die Auswahl „DATA Deneb Signaturdienst“ ausgewählt werden. Die hier benötigten Login-Daten haben Sie üblicherweise zusammen mit den Konfigurationsdaten erhalten, die Sie in der Registerkarte „Governikus“ in den Einstellungen eingegeben haben, siehe dazu auch Kapitel 5.4.

Wenn Sie den „DATA Deneb Signaturdienst“ durch Anklicken ausgewählt haben, wird der Login-Dialog für den Authentisierungsdienst angezeigt, siehe nächste Abbildung.

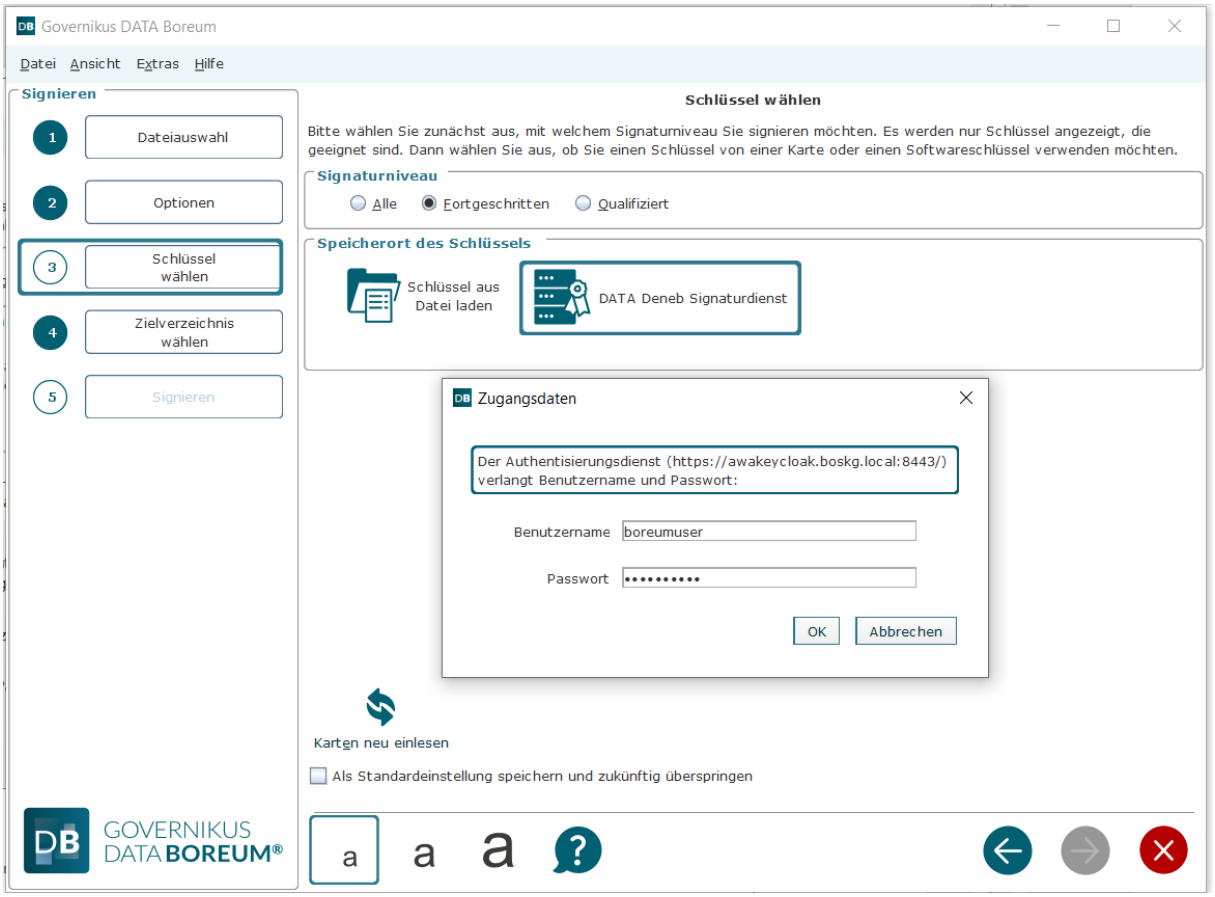

Abbildung 36: Auswahl Signaturdienst und Login-Dialog für den Authentisierungsdienst

Mit den Login-Daten verbindet sich DATA Boreum mit dem Authentisierungsdienst. Danach übergibt der Authentisierungsdienst die Anfrage an den Signaturdienst von DATA Deneb. DATA Deneb gibt die Schlüssel zurück, für die Sie autorisiert sind und DATA Boreum zeigt diese an. Sie können den Schlüssel, den Sie zum Signieren nutzen wollen, durch Anklicken auswählen.

Merkmale für die Schlüsselauswahl von DATA Deneb Signaturdienst

- **Signaturniveau festlegen**: Das Signaturniveau ist abhängig von der Auswahl des Signaturniveaus im Dialogabschnitt über der Schlüsselauswahl, siehe Kapitel 6.4.4.1 und vom verfügbaren Schlüsselmaterial. DATA Deneb kann zum Signieren auf Kartenleser mit Multisignaturkarten und auf Softwareschlüssel (Keystores) zugreifen. Im Authentisierungsserver ist hinterlegt, für welche Schlüssel Sie berechtigt sind. Nur diese werden Ihnen zur Auswahl angezeigt. Sie können für einen oder mehrere Schlüssel berechtigt sein.

- Wenn Sie das Signaturniveau „Fortgeschritten“ ausgewählt haben, werden Ihnen nur Schlüssel aus Keystores zur Auswahl angeboten, für die Sie berechtigt sind.
- Wenn Sie das Signaturniveau „Qualifiziert“ ausgewählt haben, werden Ihnen nur die Signaturzertifikate für qualifizierte elektronische Signaturen angezeigt, die auf Multisignaturkarten gespeichert, für die Sie berechtigt sind.

- **Beschränkungen**: Sie können eine Datei oder einen Stapel von Dateien zum Signieren übergeben. Ein Stapel darf nicht mehr als **500** Dateien umfassen.
- **Dauer der Schlüsselauswahl**: DATA Boreum speichert die Login-Daten im temporären Speicher (Cache). Diese Daten sind gültig, so lange DATA Boreum nicht beendet wird. Wenn Sie DATA Boreum beenden und erneut aufrufen, müssen Sie diese Login-Daten erneut eingeben.

6.4.4.2.4 BNotK Fernsignaturdienst

BNotK ist die Abkürzung für Bundesnotarkammer. Damit im Dialogabschnitt „Speicherort des Schlüssels“ der BNotK Fernsignaturdienst angezeigt wird, muss zuvor in den „Einstellungen“ in der Registerkarte „BNotK“ die Option „Ja, der Fernsignaturdienst soll verwendet werden.“ ausgewählt sein, lesen Sie dazu Kapitel 5.5.

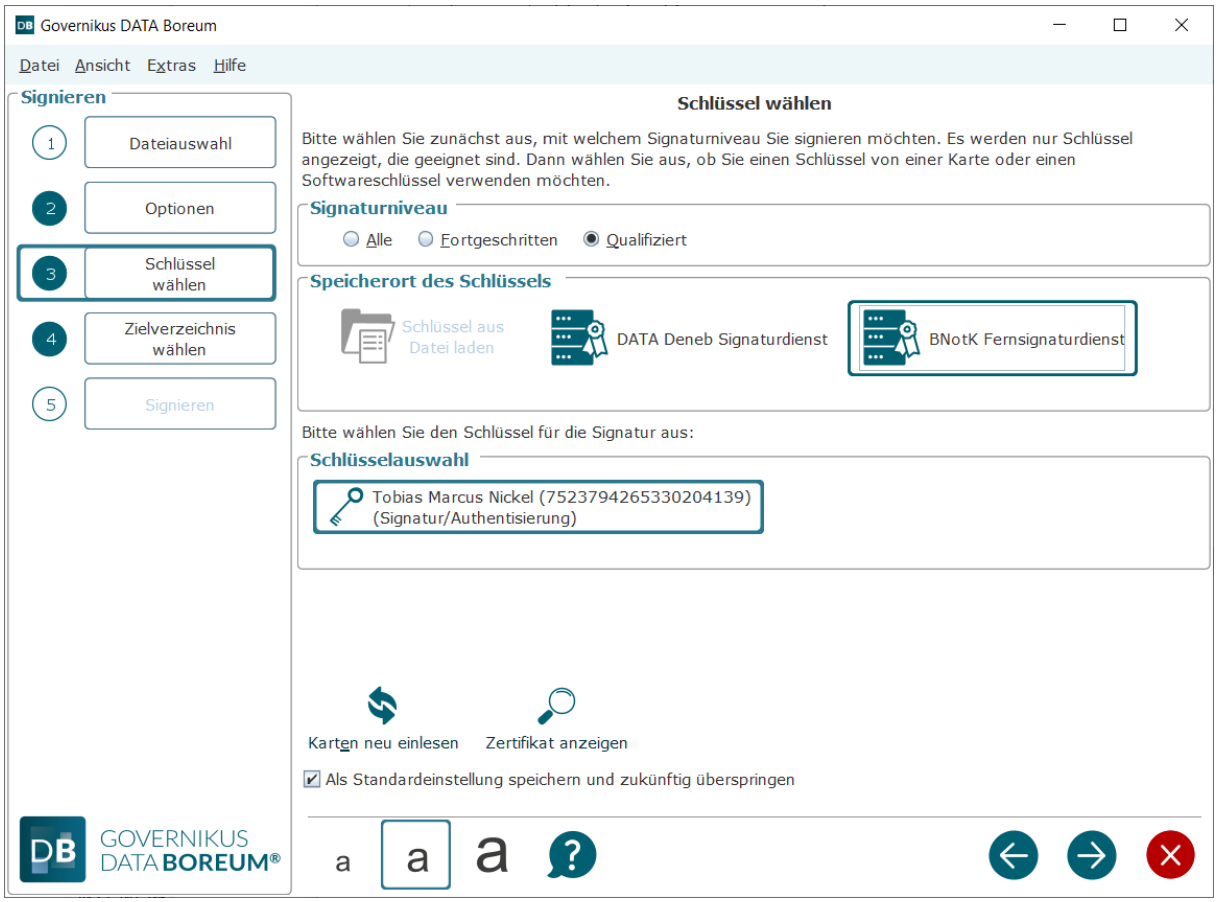

Abbildung 37: Auswahl des BNotK Fernsignaturdienstes

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 die Benutzung des BNotK Fernsignaturdienstes ausgewählt haben, wird ein möglicherweise zuvor angezeigter Button zur Auswahl eines Chipkartenlesers mit Signaturkarte nicht mehr angezeigt.

6.4.4.2.5 Schlüssel wählen

Wenn Sie einen Speicherort ausgewählt haben (Datei, Chipkartenleser, Signaturdienst, BNotK Fernsignaturdienst), 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.

6.4.4.2.6 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.

6.4.4.2.7 Standardeinstellung

Wie im Kapitel 6.3 erklärt, können Sie die auf dieser Dialogseite vorgenommen Einstellungen als Standardeinstellungen speichern. Wenn Sie zukünftig beim Signieren über die blauen Navigationspfeile rechts unten navigieren, wird diese Seite nicht mehr angezeigt. Die Standardeinstellung verfällt, wenn der zuvor als Standard gespeicherte Schlüssel nicht zur Verfügung steht.

Achtung: Nur qualifizierte elektronische Signaturen sind der eigenhändigen Unterschrift bezüglich der Rechtswirkung weitestgehend gleichgestellt.

Tastaturbefehle auf dieser Seite

- Alt + z = Das gewählte Zertifikat wird angezeigt.

6.4.5 Zielverzeichnis wählen

Das Auswählen eines Zielverzeichnisses ist im Kapitel 6.3.3 erklärt. Im Zielverzeichnis werden die elektronisch signierten Dateien abgelegt.

- **Signierte Datei enthält die Signatur**: Wenn Sie in den Optionen ausgewählt haben, dass die Signatur in die Datei integriert wird, also bei enveloping Signaturen (CAdES) oder bei PDF-Dateien (PAdES), dann wird die signierte Datei im ausgewählten Zielverzeichnis abgelegt.
- **Signatur ist in einer zusätzlichen Signaturdatei enthalten**: Wenn Sie in den Optionen ausgewählt haben, dass die Signatur in einer eigenen Signaturdatei erstellt wird, also für detached (CAdES für alle Dateitypen) oder bei detached XML-Dateien (XAdES), dann wird die Inhaltsdatendatei (also das Original) und die Signaturdatei im Zielverzeichnis abgelegt. Dadurch, dass beide Dateien im Zielverzeichnis liegen, kann auch hier beispielsweise gleich eine Weiterverarbeitung mit der Funktion Validieren durchgeführt werden. Wenn als Zielverzeichnis das Quellverzeichnis verwendet wird, ist dies sowieso gewährleistet, denn die Originaldatei liegt bereits im Quellverzeichnis.

Standardeinstellung

Wie im Kapitel 6.3 erklärt, können Sie die auf dieser Dialogseite vorgenommen Einstellungen als Standardeinstellungen speichern. Wenn Sie zukünftig beim Signieren über die blauen Navigationspfeile rechts unten navigieren, wird diese Seite nicht mehr angezeigt.

Tastaturbefehle auf dieser Seite

- Alt + q = Button "Quellverzeichnis nutzen"
- Alt + z = Button "Zielverzeichnis wählen"

6.4.6 Signieren

Dies ist die letzte Dialogseite der Signieren-Funktion. In der Liste werden alle Dateien aufgeführt, die Sie bei der Dateiauswahl (siehe Kapitel 6.3.2) ausgewählt haben. Nachdem Sie auf den Signieren-Button am unteren Rand des Dialogfensters geklickt haben, werden nacheinander alle Dateien signiert, die in der Liste aufgeführt sind.

PIN-Eingabe

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

Achtung:

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

Neue oder andere Signaturkarte

Wenn Sie eine Signaturkarte das erste Mal in Governikus DATA Boreum verwenden oder wenn Sie eine andere Signaturkarte verwenden, als die, die zuvor in Governikus DATA Boreum 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 Chipkartenleser und Governikus DATA Boreum aus Sicherheitsgründen nur verschlüsselt erfolgen darf. Es werden Verschlüsselungszertifikate zwischen dem Chipkartenleser und Governikus DATA Boreum 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 6.4.3.4, wird Ihnen nach dem Klicken auf den „Signieren“-Button der Login-Dialog für den Authentisierungsdienst angezeigt.

Hinweis: Die Login-Daten haben Sie üblicherweise zusammen mit den Konfigurationsdaten erhalten, die Sie in der Registerkarte „Governikus“ in den Einstellungen eingegeben haben, siehe dazu auch Kapitel 5.4.

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 6.4.4. 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.

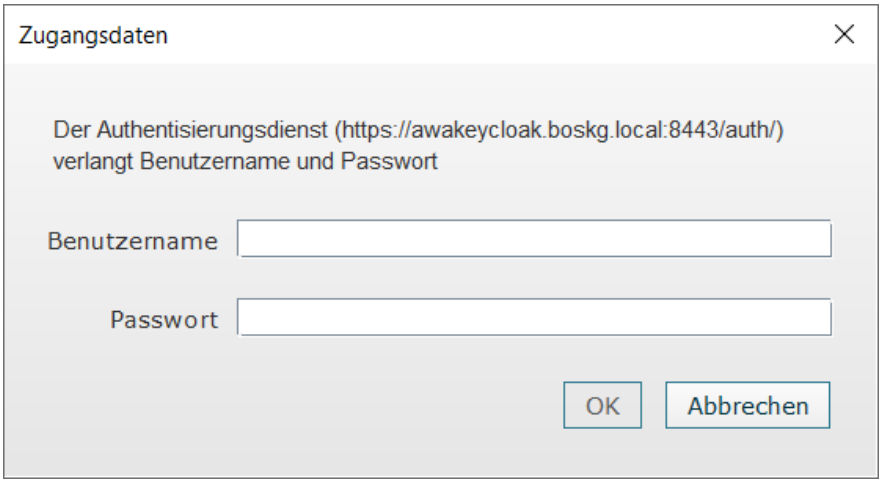

Abbildung 38: Login-Dialog für den Authentisierungsdienst

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.

	**Hinweis**: Das Anlegen von Feldern für sichtbare PDF-Signaturen kann hier über den Aufruf des Kontextmenüs in der Dateiliste erfolgen.

-  : Das Augensymbol wird angezeigt, wenn die Datei vor dem Signieren angezeigt wurde (siehe auch Kapitel 5.1, Abschnitt Mindestanzahl). Das Symbol ist grau, wenn die Datei noch nicht angezeigt wurde.
-  : Über dieses Symbol wird die Dateianzeige aufgerufen. Es das Programm für die Anzeige aufgerufen, das mit diesem Dateityp assoziiert ist, also beispielsweise das Programm "MS Word" für Dateien mit dem Suffix `docx`.
- **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:
  - **Fertig**: die Verarbeitung ist abgeschlossen;
  - **Fehler**: bei der Verarbeitung ist ein Fehler aufgetreten. Wenn Sie mit der Maus auf diesen Status zeigen, wird in einem Tooltip die Fehlerursache angezeigt.
- **Ergebnisdatei**: Bei einer erfolgreichen Verarbeitung sind in dieser Spalte der Pfad und der Dateiname der signierten Datei zu sehen.

Ergebnisdatei vorhanden

Wenn beim Erstellen der Ergebnisdatei bemerkt wird, dass eine Datei mit gleichem Namen im Zielverzeichnis bereits vorhanden ist, wird der Dialog "Datei vorhanden" angezeigt. Sie haben hier die Möglichkeit, eine Auswahl zu treffen. Sie können die Datei überschreiben oder die

Datei umbenennen lassen. Beim Umbenennen wird der Datei das aktuelle Datum im Dateinamen vorangestellt. Sie können die Verarbeitung aber auch abbrechen.

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.

Dateien mit folgendem Programm weiterverarbeiten

Benutzen Sie die Auswahlliste um ein Programm auszuwählen, mit dem die signierten Dateien weiterverarbeitet werden sollen. Die Voreinstellung ist "Keine Weiterverarbeitung". Das ausgewählte Programm wird direkt mit den signierten Dateien aufgerufen. Die Auswahlliste zeigt alle Programme an, die Sie im Dialog "Einstellungen" in der Registerkarte "Anwendungen" konfiguriert haben, siehe Kapitel 5.2.

Bitte beachten Sie, dass bei einem macOS nur die Standardfunktionen zur Verfügung stehen. Die Übergabe von Dateien an Programme, die in "Anwendungen verwalten" angegeben wurden, funktioniert bei einem macOS nicht.

Hinweis: Sie können Weiterverarbeitung auch noch **nach** der Verarbeitung der Dateien auswählen. Klicken Sie dann nach der Auswahl des Nachfolgeprogramms auf das ▶ Symbol, um die Ausführung zu starten. **Achtung**: Es werden **alle** Ergebnisdateien an das Nachfolgeprogramm übergeben.

Unterer Dialogabschnitt der Funktion Signieren

Auf dem unteren Dialogabschnitt der Funktion Signieren werden unterhalb der Dateiliste und der Auswahl des Nachfolgeprogramms die Einstellungen zusammengefasst, die Sie für diesen Signiervorgang getroffen haben. Klicken Sie auf den Signieren-Button, um den Prozess zu starten.

	**Achtung**: Oberhalb der Buttons "Signieren" werden alle Einstellungen, die Sie konfiguriert haben, zusammengefasst. Prüfen Sie, ob Sie mit diesen Einstellungen signieren wollen. Sie können die Einstellungen vor dem Signieren erneut ändern, indem Sie zur Dialogseite "Optionen" zurückkehren.

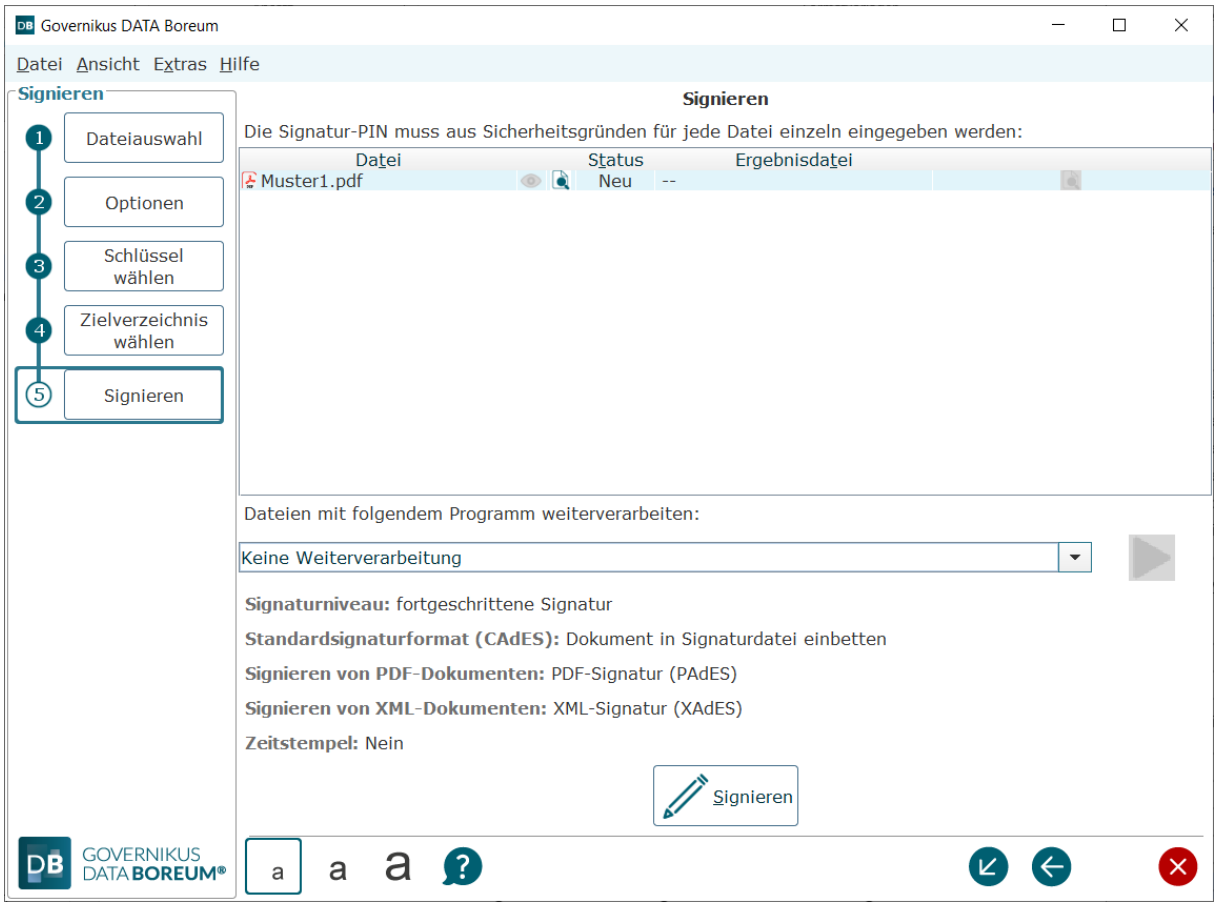

Abbildung 39: Letzte Dialogseite der Funktion Signieren

Tastaturbefehle auf dieser Seite

- Alt + Enter = Button "Signieren"

6.4.7 Sonderfälle Stapelsignaturkarte und Multisignaturkarte

Stapelsignaturkarten

Stapelsignaturkarten sind besondere Signaturkarten, die das Signieren mehrerer Dateien, typisch sind 100 Signaturen, mit einmaliger PIN-Eingabe ermöglichen. Wenn alle Dateien signiert sind und Sie im Dialog Dateiauswahl erneut Dateien zur Signatur auswählen, muss die PIN allerdings erneut eingegeben werden.

Multisignaturkarten

Multisignaturkarten sind besondere Signaturkarten für die "Massensignatur", die eine unbegrenzte Anzahl von Signaturen pro PIN-Eingabe ermöglichen. Governikus DATA Boreum unterstützt diese Signaturkarten, jedoch nur analog der Stapelsignaturkarte. Für jeden

Signaturvorgang muss mindestens einmal die PIN eingegeben werden. Die Anzahl der Signaturen pro PIN-Eingabe ist durch Governikus DATA Boreum auf 500 Signaturen begrenzt.

Einzelne QES mit Stapelsignaturkarte oder Multisignaturkarte

Wenn Sie die Funktion Signieren aufrufen und genau **ein** Dokument an Governikus DATA Boreum übergeben, kann auch mit einer Stapelsignaturkarte oder mit einer Multisignaturkarte nach der PIN-Eingabe **nur eine** qualifizierte elektronische Signatur (QES) erstellt werden. Danach ist der Signaturvorgang aus Sicherheitsgründen beendet und die jeweilige Karte kann nur nach erneuerter PIN-Eingabe zur Anbringung weiterer Signaturen verwendet werden.

Mehrfache QES mit Stapelsignaturkarte oder Multisignaturkarte

Wenn Sie mehrere Dateien an Governikus DATA Boreum übergeben, können Sie mit einer Stapelsignaturkarte oder mit einer Multisignaturkarte mit einmaliger PIN-Eingabe für die übergebenen Dokumente mehrere qualifizierte elektronische Signaturen (QES) erstellen. Es werden bis zu Kartenlimit Signaturen angebracht. Die PIN-Eingabe gilt immer nur für die Menge der aktuell an Governikus DATA Boreum übergebenen Dokumente. Jede neue Übergabe von Dokumenten an Governikus DATA Boreum erfordert die erneute Eingabe der PIN.

Wenn Sie mit einer Stapelsignaturkarte signieren und übergeben mehr als hundert Dokumente, müssen Sie nach hundert Signaturen die PIN erneut eingeben. Dasselbe gilt analog für Multisignaturkarten und das Limit von 500 Signaturen.

Achtung: Bitte beachten Sie, dass für die Verwendung von Stapel- und Multisignaturkarten besondere Sicherheitsanforderungen wie der physische Schutz gegen unbefugten Zugriff zur SSEE, insbesondere bei einem unbeaufsichtigten Betrieb gelten.

Bitte beachten Sie hierzu bitte unbedingt die Auflagen des Kartenherausgebers hinsichtlich der Nutzung der Multisignaturkarte.

6.5 Validieren

Was wird validiert?

In diesem Dialog können Sie elektronisch signierte Dateien, Zertifikatsdateien und Zeitstempeldateien validieren. Eine Erklärung zum Validieren finden Sie im Anhang "Erläuterungen" im Kapitel 9.7.

Aufruf

Klicken Sie auf der Einstiegsseite von Governikus DATA Boreum auf "Validieren", benutzen Sie alternativ das Tastaturkürzel " Strg + 2".

Aufruf mit Datei

Hinweis: Für macOS Benutzer steht das Kontextmenü nicht zur Verfügung.

Direktes Validieren über Kontextmenü

Sie können Dateien im Dateimanager auswählen und aus dem Kontextmenü "Validieren" wählen. Sollte Governikus DATA Boreum noch nicht gestartet sein, so wird er mit Ihrer

Auswahl gestartet. Sollte Governikus DATA Boreum bereits gestartet sein und Sie wählen eine Datei über das Kontextmenü, so ersetzt die ausgewählte Datei alle Dateien, die möglicherweise bereits zuvor ausgewählt waren.

Hinweis: Wenn Sie Dateien validieren möchten, die im Format CAdES detached vorliegen, also Signatur und signierter Inhalt in separaten Dateien, fügen Sie über das Kontextmenü bitte nur die Signaturdatei (Endung z.B. .p7s) hinzu.

6.5.1 Signaturformate

Für elektronische Signaturen existieren unterschiedliche Standards. Im Kapitel 9.5 gibt es zu einigen Signaturformaten Erläuterungen. Die Validierungsfunktion von Governikus DATA Boreum unterstützt die folgenden Formate:

- **CAdES:** CAdES steht für **C**MS **Ad**vanced **E**lectronic **S**ignatures. Die typische Dateiendung von CAdES-Signaturdateien ist `p7s`. Unterstützt werden diese beiden Ausprägungen:
  - **enveloped**: Der signierte Inhalt ist in der Signaturdatei enthalten.
  - **detached**: Die Signatur liegt in einer separaten Datei vor. Wenn eine Signatur in der Ausprägung detached validiert werden soll, müssen die Originaldatei und die Signaturdatei vorliegen.

Hinweis: Es wird geprüft, ob die Originaldatei den gleichen Namen hat wie die Signaturdatei (natürlich ohne das Suffix `p7s`). Beispiel:

Inhaltsdatendatei: `test.docx`

Signaturdatei: `test.docx.p7s`

Validiert wird von beiden Dateien jedoch nur die bestehende Signaturdatei. Nach dem Auswählen der Signaturdatei werden Sie dazu aufgefordert die Originaldatei auszuwählen. Auf der Dialogseite Dateiauswahl wird anschließend nur die Signaturdatei angezeigt.

- **PDF** (PDF-Inline/PAdES): Bei einer PDF-Signatur ist die Signatur im signierten PDF-Dokument enthalten. Die signierte PDF-Datei trägt weiter die Endung `.pdf` und kann mit beliebigen PDF-Anzeigeprogrammen angezeigt werden. Eine PDF-Datei kann auch mehrere Signaturen enthalten.
- **XML** (XAdES): Es können XML-Dateien geprüft werden, bei denen eine Signatur gemäß dem Standard XAdES (**X**ML **Ad**vanced **E**lectronic **S**ignatures) erstellt wurde. Wurde die Signatur enveloped erstellt, so wurde sie über die gesamte XML-Datei gebildet. Auch detached XML-Signaturen werden unterstützt.
- **S/MIME:** Der Standard S/MIME (Secure/Multipurpose Internet Mail Extensions) gilt für signierte E-Mails. E-Mails die in Form einer "electronic mail"-Datei (Endung `.eml`) vorliegen können geprüft werden. Es kann nur die Signatur geprüft werden. Signierte Anhänge müssen separat validiert werden.
- **MS Outlook-Mail**: Das E-Mail-Dateiformat `msg` ist ein eigenes Dateiformat der Microsoft Corporation. E-Mails, die aus dem Mail-Client Microsoft Outlook gespeichert werden, haben die Dateiendung `msg`. Governikus DATA Boreum unterstützt die Validierung für E-Mail-Dateien der Versionen Outlook 2007, Outlook 2010, Outlook 2013 und Outlook 2016. E-Mails aus älteren Outlook-Versionen müssen vor einer Prüfung in das `eml`-

Format konvertiert werden. Es kann nur die Signatur geprüft werden. Signierte Anhänge müssen separat validiert werden.

- **De-Mail:** Signierte De-Mail-Nachrichten oder De-Mail-Bestätigungsnachrichten, die in Form einer "electronic mail"-Datei (Endung `eml`) vorliegen, können validiert werden. Es kann nur die Signatur geprüft werden. Signierte Anhänge müssen separat validiert werden.
- **Zertifikat:** Separat vorliegende Zertifikate nach X.509v3-Standard können auch unabhängig von einer Signatur auf Gültigkeit geprüft werden. Die typischen Dateiendungen sind `cer` und `crt`.
- **Associated Signature Containers (ASiC)**: Das European Telecommunications Standards Institute (ETSI) hat einen Europäischen Standard für eine signierte Container-Struktur (ASiC) herausgegeben. ASiC benutzt als Container-Struktur das ZIP-Dateiformat. Die enthaltenen Signaturformate sind CAdES oder XAdES. Signierte Associated-Signature-Container-Dateien haben die Dateiendung `scs`, `sce`, `asics`, oder `asice`.

Bezugsquellen: Weitere Detail-Informationen und Hinweise zu den unterstützten Signaturformaten finden Sie in dem Dokument "Governikus-Prüfprotokoll" im Anhang.

6.5.2 Dateiauswahl

Wählen Sie hier die Dateien aus, die Sie validieren wollen. Die Dateiauswahl ist in Kapitel 6.3.2 erklärt.

Die Dateiliste

Die Dateiliste zeigt zeilenweise die von Ihnen zum Validieren ausgewählten Dateien.

Tastaturbefehle auf dieser Seite

- Alt + a = Datei hinzufügen
- Entf = Ausgewählte Dateien entfernen
- Alt + t = Fokus in die Tabelle setzen

6.5.3 Optionen für die Funktion Validieren

Beim Validieren wird die signierte Datei immer lokal auf Integrität geprüft. Damit kann nachgewiesen werden, dass die Datei nach dem Signieren nicht verändert wurde. Auf dieser Dialogseite können Sie folgende Einstellungen vornehmen.

Validierungsdienst konfigurieren

Über den Link „Validierungsdienst konfigurieren“ gelangen Sie in den Dialog „Einstellungen“. Es wird die Registerkarte zum Konfigurieren des Validierungsdienstes angezeigt, die im Kapitel 5.7 erklärt ist.

Zielverzeichnis Prüfprotokoll

Die Auswahl eines Zielverzeichnisses geschieht so, wie im Kapitel 6.3.3 beschrieben.

Standardeinstellung

Wie im Kapitel 6.3 erklärt, können Sie die auf dieser Dialogseite vorgenommen Einstellungen als Standardeinstellungen speichern. Wenn Sie zukünftig beim Validieren über die blauen Navigationspfeile rechts unten navigieren, wird diese Seite nicht mehr angezeigt.

Tastaturbefehle auf dieser Seite

- Alt + q = Button "Quellverzeichnis nutzen"
- Alt + z = Button "Zielverzeichnis wählen"

6.5.4 Validieren

Dies ist das letzte Dialogfenster der Funktion Validieren. In der Liste werden alle Dateien aufgeführt, die Sie bei der Dateiauswahl (siehe Kapitel 6.3.2) ausgewählt haben. Nachdem Sie auf den Validieren-Button am unterhalb der Dateiliste geklickt haben, werden nacheinander alle Dateien validiert, die in der Liste aufgeführt sind.

Hinweis: Über dem Validieren-Button wird die URL zum Validierungsdienst angezeigt, die Sie im Einstellungsdialog konfiguriert haben. Bitte überprüfen Sie vor dem Validieren, ob diese Angabe stimmt oder, ob diese Einstellung möglicherweise manipuliert wurde.

Sonderfall Zertifikatsdateien validieren

Zertifikatsdateien werden zum Signieren, zum Verschlüsseln und zum Entschlüsseln benutzt. Sie können mit der Funktion "Validieren" auch Zertifikatsdateien validieren, um Auskunft über deren Gültigkeit zu bekommen. Diese haben üblicherweise die Dateiendung `.cer` oder `.crt`. Wenn Sie über den Dialog Dateiauswahl eine Zertifikatsdatei geladen haben und klicken auf der letzten Seite der Funktion auf den "Validieren"-Button, wird Ihnen ein Dialog zum Prüfzeitpunkt angezeigt. Bitte beachten Sie, dass dieser Dialog nur beim Validieren von Zertifikatsdateien angezeigt wird.

Als Prüfzeitpunkt ist das aktuelle Datum ausgewählt. Sie können den Prüfzeitpunkt anpassen. Geprüft wird, ob das Zertifikat zum angegebenen Zeitpunkt gültig war.

- **Aktueller Zeitpunkt**: Wenn diese Checkbox ausgewählt ist, wird die aktuelle Zeit als Prüfzeitpunkt genutzt. Nur wenn Sie diese Checkbox abwählen, können Sie ein anderes Datum angeben.
- **OK**: Wenn Sie den Dialog mit OK bestätigen, wird der von Ihnen eingestellte Prüfzeitpunkt benutzt. Wenn Sie mehrere Zertifikatsdateien in der Dateiliste haben, wird der ausgewählte Prüfzeitpunkt für alle Zertifikatsdateien in der Liste benutzt. Es erfolgt keine erneute Abfrage.
- **Abbrechen**: Wenn Sie den Dialog mit dem X oben rechts im Dialogfenster abbrechen, wird die aktuelle Zeit zur Prüfung der Zertifikatsdatei benutzt. Wenn Sie mehrere Zertifikatsdateien geladen haben, wird die Abfrage des Prüfzeitpunkts bei der nächsten Zertifikatsdatei erneut angezeigt.

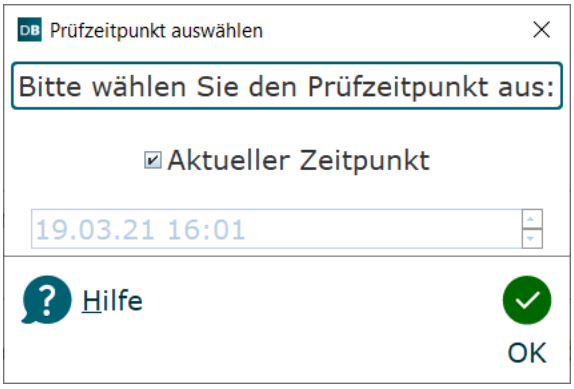

Abbildung 40: Dialogfenster Prüfzeitpunkt auswählen

Die Listendarstellung

Die Zeilen in der Listendarstellung haben die folgenden Spalten:

- **Datei**: Zeigt den Namen der Dateien an, die Sie zum Validieren 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:
  - **Fertig**: die Verarbeitung ist abgeschlossen;
  - **Fehler**: bei der Verarbeitung ist ein Fehler aufgetreten. Wenn Sie mit der Maus auf diesen Status zeigen, wird in einem Tooltip die Fehlerursache angezeigt.
- **Ergebnisdatei**: Das Ergebnis des Validierens ist ein Prüfprotokoll für jede validierte Datei. Das Prüfprotokoll wird als HTML- oder PDF-Datei im Zielverzeichnis gespeichert, Einstellung siehe Kapitel 5.7. Das Prüfprotokoll ist in Kapitel 6.5.5 beschrieben. Bei einer erfolgreichen Verarbeitung sind in dieser Spalte Pfad und Dateiname des Prüfprotokolls zu sehen. Visualisierung des Prüfergebnisses:
  - : Der grüne Kreis mit dem OK-Haken zeigt an, dass alle Prüfungen ein positives Ergebnis geliefert haben.
  - : Der gelbe Kreis mit dem Ausrufezeichen zeigt an, dass mindestens eine Prüfung nicht durchgeführt werden konnte.
  - : Der rote Kreis mit dem Kreuz zeigt an, dass mindestens eine Prüfung ein negatives Ergebnis geliefert hat.
- : Wenn sie auf dieses Symbol ganz rechts in der Zeile klicken, wird das Prüfprotokoll angezeigt. Wenn Sie unter "Extras - Einstellungen - Registerkarte Validieren" PDF als Format für das Prüfprotokoll gewählt haben, wird der PDF-Viewer aufgerufen, der für PDF-Dateien auf ihrem Computer registriert ist. Wenn Sie HTML als Format für das Prüfprotokoll gewählt haben, wird es in Ihrem bevorzugten Web-Browser angezeigt.

Ergebnisdatei vorhanden

Wenn beim Erstellen der Ergebnisdatei bemerkt wird, dass eine Datei mit gleichem Namen im Zielverzeichnis bereits vorhanden ist, wird der Dialog "Datei vorhanden" angezeigt. Sie haben hier die Möglichkeit, eine Auswahl zu treffen. Sie können die Datei überschreiben oder die

Datei umbenennen lassen. Beim Umbenennen wird der Datei das aktuelle Datum im Dateinamen vorangestellt. Sie können die Verarbeitung aber auch abbrechen.

Dateien mit folgendem Programm weiterverarbeiten bzw. drucken

Benutzen Sie die Auswahlliste um ein Programm auszuwählen, mit dem das Prüfprotokoll weiterverarbeitet werden soll oder ob das Prüfprotokoll gedruckt werden soll. Die Voreinstellung ist "Keine Weiterverarbeitung". Das ausgewählte Programm wird direkt mit den signierten Dateien aufgerufen. Die Auswahlliste zeigt alle Programme an, die Sie im Dialog "Einstellungen" in der Registerkarte "Anwendungen" konfiguriert haben, siehe Kapitel 5.2.

Bitte beachten Sie, dass bei einem macOS nur die Standardfunktionen zur Verfügung stehen. Die Übergabe von Dateien an Programme, die in "Anwendungen verwalten" angegeben wurden, funktioniert bei einem macOS nicht.

Hinweis: Sie können Weiterverarbeitung auch noch **nach** der Verarbeitung der Dateien auswählen. Klicken Sie dann nach der Auswahl des Nachfolgeprogramms auf das ▶ Symbol, um die Ausführung zu starten. **Achtung**: Es werden **alle** Ergebnisdateien an das Nachfolgeprogramm übergeben.

Letzte Dialogseite der Funktion Validieren

Auf der letzten Dialogseite der Funktion Validieren werden unterhalb der Dateiliste und der Auswahl des Nachfolgeprogramms die Einstellungen zusammengefasst, die Sie für diese Funktion getroffen haben. Es wird die URL des Validierungsdienstes angezeigt. Sollten Sie keinen Validierungsdienst konfiguriert haben, wird die Meldung "Onlineprüfung ist abgewählt" angezeigt. Klicken Sie auf den Validieren-Button, um den Prozess zu starten.

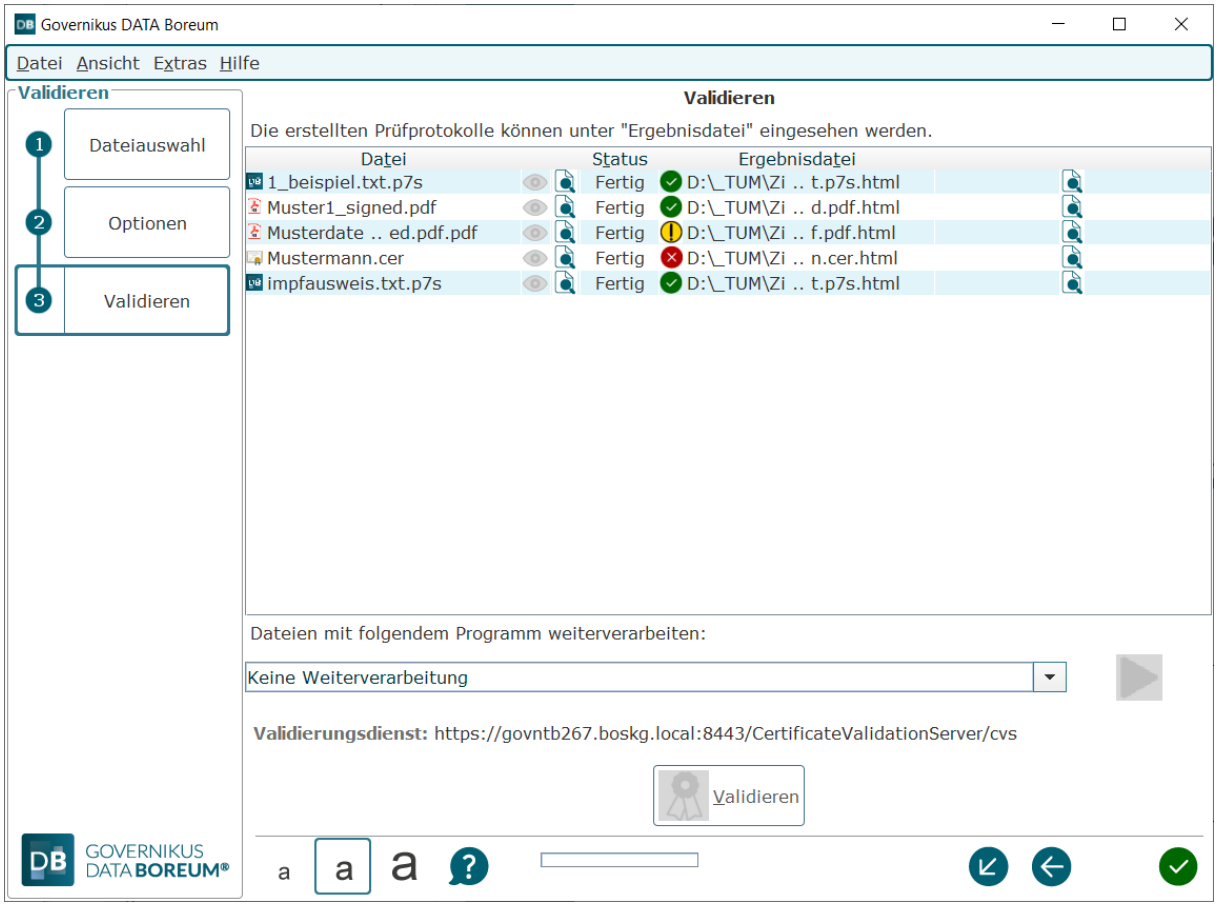

Abbildung 41: Letzte Dialogseite der Funktion Validieren

Tastaturbefehle auf dieser Seite

- Alt + t = Fokus in die Tabelle setzen
- Alt + Enter = Button "Validieren"

6.5.5 Das Prüfprotokoll

Das Ergebnis des Validierens ist ein Prüfprotokoll, das als HTML- oder PDF-Datei oder auch als XML (Einstellung siehe Kapitel 5.7) im Zielverzeichnis gespeichert wird. Das Prüfprotokoll zeigt Ihnen, welche Prüfungsschritte ein positives oder ein negatives Ergebnis lieferten oder ob ein Prüfungsschritt nicht durchgeführt werden konnte. Eine Beschreibung des Prüfprotokolls (HTML) finden Sie im Dokument `Governikus-Pruefprotokoll.pdf`, das Teil der Auslieferung ist.

Das Prüfprotokoll, das von DATA Boreum nach einer Validierung zur Verfügung gestellt wird, kann auch als XML-Datei ausgegeben werden. Dieses XML-Prüfprotokoll ist ETSI konform und wird auch ETSI SVR XML-Prüfprotokoll genannt.

ETSI-Signature Validation Report (SVR): Maschinenlesbares XML-Prüfprotokoll, spezifiziert von ETSI in der EN 319 102-2. Zurzeit als TS 119 102-2 in der Version 1.2.1 unterstützt. Der Standard wurde von ETSI im Rahmen des Normierungsmandats M/460 zur technischen Umsetzung der rechtlichen Anforderungen aus der eIDAS-Verordnung spezifiziert.

Das Protokoll enthält einen Gesamtstatus (total-passed, total-failed, indeterminate) für jede validierte Signatur und das ermittelte Niveau der Signatur. Im Fehlerfall und bei unbestimmten Status wird zur näheren Beschreibung die in der ETSI EN 319102-1 definierte Subindication

zurückgemeldet. Zusätzlich wird eine URI ausgegeben, die auf den Meldungstext aus dem menschenlesbaren Protokoll verweist.

	**Bezugsquellen**: Der Standard kann über die ETSI-Seite https://www.etsi.org/standards heruntergeladen werden. Auf der Seite über die Suchmaske nach dem Standard suchen und herunterladen. Am Ende des Dokuments befindet sich auch ein Link für den Download des Schemas.

6.6 Verschlüsseln

In diesem Dialog können Sie Dateien verschlüsseln. Eine Erklärung zum Verschlüsseln finden Sie im Anhang "Erläuterungen" im Kapitel 9.8.

Aufruf

Klicken Sie auf der Einstiegsseite von Governikus DATA Boreum auf "Verschlüsseln", benutzen Sie alternativ das Tastaturkürzel " Strg + 3".

Aufruf mit Datei

Hinweis: Für macOS Benutzer steht das Kontextmenü nicht zur Verfügung.

Direktes Verschlüsseln über Kontextmenü

Sie können Dateien im Dateimanager auswählen und aus dem Kontextmenü "Verschlüsseln" wählen. Sollte Governikus DATA Boreum noch nicht gestartet sein, so wird er mit Ihrer Auswahl gestartet. Sollte Governikus DATA Boreum bereits gestartet sein und Sie wählen eine Datei über das Kontextmenü, so ersetzt die ausgewählte Datei alle Dateien, die möglicherweise bereits zuvor ausgewählt waren.

6.6.1 Dateiauswahl

Wählen Sie hier die Dateien aus, die Sie verschlüsseln wollen. Die Dateiauswahl ist in Kapitel 6.3.2 erklärt.

Die Dateiliste

Die Dateiliste zeigt zeilenweise die von Ihnen zum Verschlüsseln eingefügten Dateien. Dabei haben die Spalten diese Bedeutung:

- **Datei**: Zeigt den Dateinamen an. Wenn Sie den Mauszeiger über den Dateinamen legen, wird der vollständige Pfad angezeigt.
- : Dieses Symbol wird angezeigt, wenn die Datei vor dem Verschlüsseln angezeigt wurde. Das Symbol ist grau, wenn die Datei nicht angezeigt wurde.
- : Dieses Symbol befindet sich in der letzten Spalte jeder Zeile. Über dieses Symbol wird die unter "Datei" aufgeführte Datei angezeigt.

Tastaturbefehle auf dieser Seite

- Alt + a = Datei hinzufügen

- Entf = Ausgewählte Dateien entfernen
- Alt + t = Fokus in die Tabelle setzen

6.6.2 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.

Verschlüsselung mit Passwort

Wenn Sie die Verschlüsselung mit einem Passwort auswählen, werden Sie auf der letzten Dialogseite "Verschlüsseln" zur Eingabe eines Passworts aufgefordert. Für diese Verschlüsselung steht nur der Algorithmus "AES-256-GCM" zur Verfügung.

	**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.

	**Hinweis**: Bitte beachten Sie, dass zum Verschlüsseln nur DER-codierte Schlüssel unterstützt werden. Schlüssel mit einer anderen Codierung (bspw. base64) müssen vor der Verwendung umcodiert werden (bspw. durch Abspeichern mit DER-Kodierung).

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 den 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 9.8 über asymmetrische Verschlüsselung.

	**Hinweis**: Nach dem Laden eines Zertifikats aus einem Keystore müssen Sie die PIN für den Zugriff auf diesen Keystore eingeben. Solange das Zertifikat aus dem Keystore in der Liste enthalten ist, ist diese PIN-Eingabe auch jeweils nach dem Start von Governikus DATA Boreum einzugeben Das Laden eines Zertifikats von einer Signaturkarte hingegen erfordert keine PIN-Eingabe.

-  **Signaturkarte**: Diese Auswahl wird nur angezeigt, wenn Sie einen Chipkarten-leser angeschlossen und eine Signaturkarte eingelegt haben. Unter diesem Symbol steht der Name des Chipkartenlesers, der von Governikus DATA Boreum erkannt wurde. Sie können bis zu 10 Chipkartenleser anschließen. Sollten Sie weitere Chipkartenleser 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 Chipkartenlesern **ausgegraut**, sind diese **nicht** auswählbar. Wenn Sie eine Signaturkarte benutzen wollen, müssen Sie diese in einen angeschlossenen Chipkartenleser einlegen. Wenn die Signaturkarte vom Chipkartenleser 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 können. 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 diesem öffentlichen 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. Die Auswahl der Schlüssel können Sie genauso vornehmen wie die Auswahl von Dateien, die in Kapitel 6.3.2 erklärt ist. 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 9.8 für weitere Informationen zum Verschlüsseln.

Standardeinstellung

Wie im Kapitel 6.3 erklärt, können Sie die auf dieser Dialogseite vorgenommen Einstellungen als Standardeinstellungen speichern. Wenn Sie zukünftig beim Verschlüsseln über die blauen Navigationspfeile rechts unten navigieren, wird diese Seite nicht mehr angezeigt.

Tastaturbefehle auf dieser Seite

- Enter = Wenn der Fokus in der Tabelle ist: Gewähltes Zertifikat anzeigen.
- Entf = Markierte Zertifikate entfernen

- Alt + t = Fokus in die Tabelle setzen

6.6.3 Zielverzeichnis wählen

Das Auswählen eines Zielverzeichnisses ist im Kapitel 6.3.3 erklärt. Im Zielverzeichnis werden die verschlüsselten Dateien abgelegt.

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`.

Standardeinstellung

Wie im Kapitel 6.3 erklärt, können Sie die auf dieser Dialogseite vorgenommen Einstellungen als Standardeinstellungen speichern. Wenn Sie zukünftig beim Verschlüsseln über die blauen Navigationspfeile rechts unten navigieren, wird diese Seite nicht mehr angezeigt.

Tastaturbefehle auf dieser Seite

- Alt + q = Button "Quellverzeichnis nutzen"
- Alt + z = Button "Zielverzeichnis wählen"

6.6.4 Verschlüsseln

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

Zufallszahlenerzeugung

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

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

Die Listendarstellung

Die Zeilen in der Listendarstellung haben die folgenden Spalten:

- **Datei**: Zeigt den Namen der Datei an, die verschlüsselt werden soll. Wenn Sie den Mauszeiger über den Dateinamen legen, wird der vollständige Pfad angezeigt.
-  : Das Augensymbol wird angezeigt, wenn die Datei vor dem Verschlüsseln angezeigt wurde. Das Symbol ist grau, wenn die Datei noch nicht angezeigt wurde.

-  : Über dieses Symbol wird die Dateianzeige mit der unter "Datei" aufgeführten Datei aufgerufen.
- **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. Wenn Sie mit der Maus auf diesen Status zeigen, wird in einem Tooltip die Fehlerursache angezeigt.
- **Ergebnisdatei**: Das Ergebnis des Verschlüsselns ist eine Datei mit der Endung `p7m`. bei einer Verschlüsselung mit Zertifikat bzw. der Endung `enz` bei der Verschlüsselung mit Passwort. 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.

	**Hinweis**: Bitte beachten Sie, dass die Ergebnisdatei der Verschlüsselung mit Passwort zusätzlich die Dateiendung `enz` hat. Es handelt sich dabei um ein passwortgeschütztes Archivformat, dass Sie mit der Entschlüsselungsfunktion von Governikus DATA Boreum wieder in die ursprüngliche Datei zurück wandeln können.

- **Hinweis**: Das Anzeigen von verschlüsselten Dateien ist nicht möglich.

Dateien mit folgendem Programm weiterverarbeiten

Benutzen Sie die Auswahlliste um ein Programm auszuwählen, mit dem die verschlüsselten Dateien weiterverarbeitet werden sollen. Die Voreinstellung ist "Keine Weiterverarbeitung". Das ausgewählte Programm wird direkt mit den signierten Dateien aufgerufen. Die Auswahlliste zeigt alle Programme an, die Sie im Dialog "Einstellungen" in der Registerkarte "Anwendungen" konfiguriert haben, siehe Kapitel 5.2.

 Bitte beachten Sie, dass bei einem macOS nur die Standardfunktionen zur Verfügung stehen. Die Übergabe von Dateien an Programme, die in "Anwendungen verwalten" angegeben wurden, funktioniert bei einem macOS nicht.

	**Hinweis**: Sie können Weiterverarbeitung auch noch **nach** der Verarbeitung der Dateien auswählen. Klicken Sie dann nach der Auswahl des Nachfolgeprogramms auf das  Symbol, um die Ausführung zu starten. **Achtung**: Es werden **alle** Ergebnisdateien an das Nachfolgeprogramm übergeben.

Ergebnisdatei vorhanden

Wenn beim Erstellen der Ergebnisdatei bemerkt wird, dass eine Datei mit gleichem Namen im Zielverzeichnis bereits vorhanden ist, wird der Dialog "Datei vorhanden" angezeigt. Sie haben hier die Möglichkeit, eine Auswahl zu treffen. Sie können die Datei überschreiben oder die Datei umbenennen lassen. Beim Umbenennen wird der Datei das aktuelle Datum im Dateinamen vorangestellt. Sie können die Verarbeitung aber auch abbrechen.

Letzte Dialogseite der Funktion Verschlüsseln

Auf der letzten Dialogseite der Funktion Verschlüsseln wird unterhalb der Dateiliste die Auswahl des Nachfolgeprogramms angezeigt. Klicken Sie auf den Verschlüsseln-Button, um den Prozess zu starten.

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, es beispielsweise nur Zahlen und zu wenig Zeichen enthält, 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.

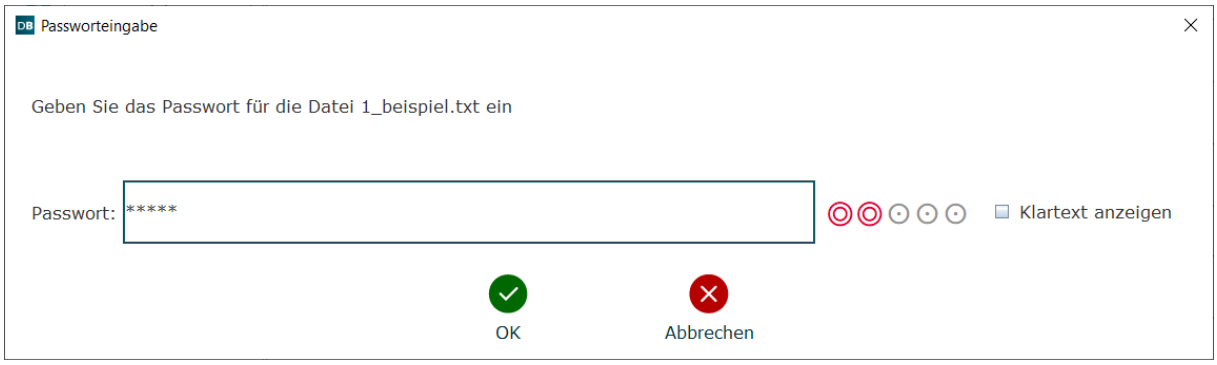

Abbildung 42: Eingabe eines trivialen Passworts - wenige rote Punkte

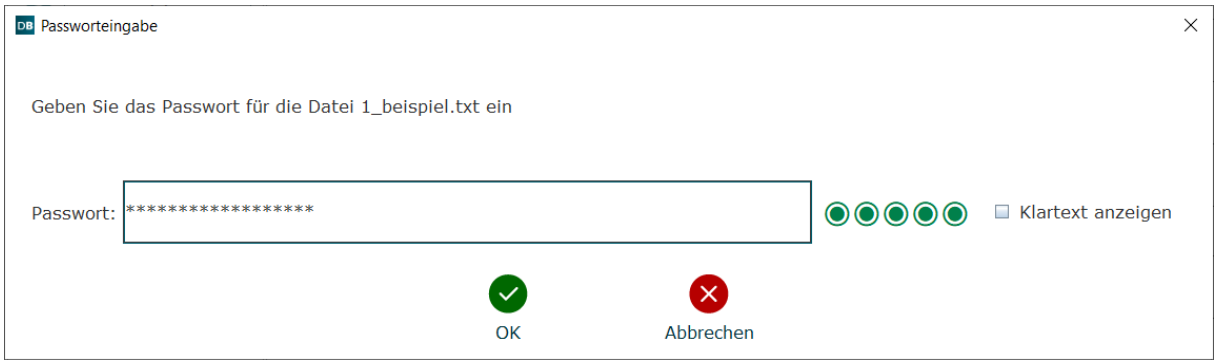

Abbildung 43: Eingabe eines ausreichend sicheren Passworts - alle Punkte grün

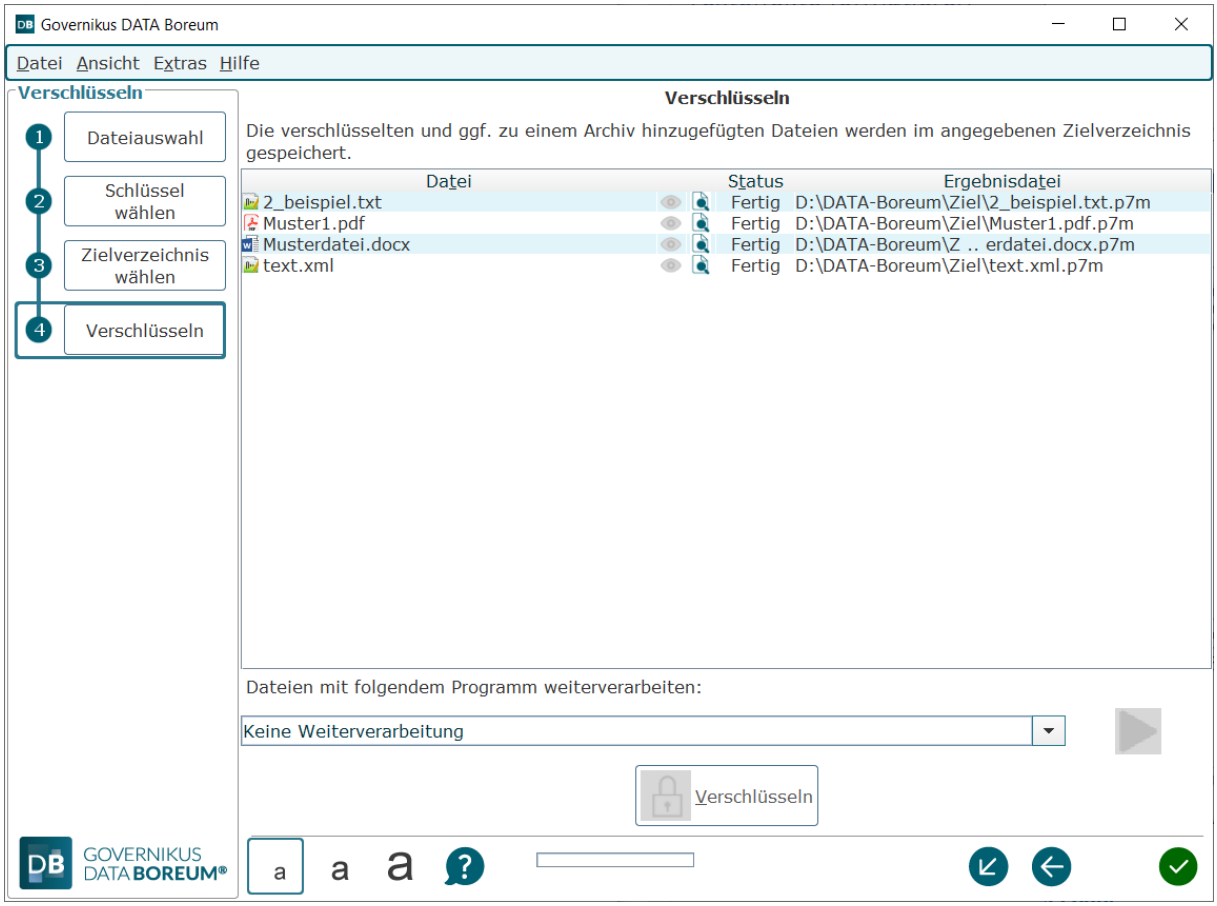

Abbildung 44: Letzte Dialogseite der Funktion Verschlüsseln

Tastaturbefehle auf dieser Seite

- Alt + t = Fokus in die Tabelle setzen
- Alt + Enter = Button "Verschlüsseln"

6.7 Entschlüsseln

In diesem Dialog können Sie Dateien entschlüsseln. Eine Erklärung zum Entschlüsseln finden Sie im Anhang "Erläuterungen" im Kapitel 9.2.

Aufruf

Klicken Sie auf der Einstiegsseite von Governikus DATA Boreum auf "Entschlüsseln", benutzen Sie alternativ das Tastaturkürzel " Strg + 4".

Aufruf mit Datei

Hinweis: Für macOS Benutzer steht das Kontextmenü nicht zur Verfügung.

Direktes Entschlüsseln über Kontextmenü

Sie können Dateien im Dateimanager auswählen und aus dem Kontextmenü "Entschlüsseln" wählen. Sollte Governikus DATA Boreum noch nicht gestartet sein, so wird er mit Ihrer Auswahl gestartet. Sollte Governikus DATA Boreum bereits gestartet sein und Sie wählen eine

Datei über das Kontextmenü, so ersetzt die ausgewählte Datei alle Dateien, die möglicherweise bereits zuvor ausgewählt waren.

6.7.1 Dateiauswahl

Wählen Sie hier die Dateien aus, die Sie entschlüsseln wollen. Die Dateiauswahl ist in Kapitel 6.3.2 erklärt. Die Dateiliste zeigt zeilenweise die von Ihnen zum Entschlüsseln eingefügten Dateien. Das Anzeigen der noch verschlüsselten Dateien ist nicht möglich.

Tastaturbefehle auf dieser Seite

- Alt + a = Datei hinzufügen
- Entf = Ausgewählte Dateien entfernen
- Alt + t = Fokus in die Tabelle setzen

6.7.2 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 Sie 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 9.8 über asymmetrische Verschlüsselung.

-  **Signaturkarte**: Diese Auswahl wird nur angezeigt, wenn Sie einen Chipkarten-leser angeschlossen und eine Signaturkarte eingelegt haben. Unter diesem Symbol steht der Name des Chipkartenlesers, der von Governikus DATA Boreum erkannt wurde. Sie können bis zu 10 Chipkartenleser anschließen. Sollten Sie weitere Chipkartenleser 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 Chipkartenlesern **ausgegraut**, sind diese **nicht** auswählbar. Wenn Sie eine Signaturkarte benutzen wollen, müssen Sie diese in einen angeschlossenen Chipkartenleser einlegen. Wenn die Signaturkarte vom Chipkartenleser 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.
  - Über den Button  können Sie direkt eine Online-Prüfung des Zertifikats durchführen. Das Prüfprotokoll wird in einem separaten Fenster angezeigt.

Standardeinstellung

Wie im Kapitel 6.3 erklärt, können Sie die auf dieser Dialogseite vorgenommen Einstellungen als Standardeinstellungen speichern. Wenn Sie zukünftig beim Entschlüsseln über die blauen Navigationspfeile rechts unten navigieren, wird diese Seite nicht mehr angezeigt.

Tastaturbefehle auf dieser Seite

Alt + z = Das gewählte Zertifikat wird angezeigt.

6.7.3 Zielverzeichnis wählen

Das Auswählen eines Zielverzeichnisses ist im Kapitel 6.3.3 erklärt. Im Zielverzeichnis werden die entschlüsselten Dateien abgelegt.

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 der Inhalt des Archivs direkt im Zielverzeichnis entpackt.

Standardeinstellung

Wie im Kapitel 6.3 erklärt, können Sie die auf dieser Dialogseite vorgenommen Einstellungen als Standardeinstellungen speichern. Wenn Sie zukünftig beim Entschlüsseln über die blauen Navigationspfeile rechts unten navigieren, wird diese Seite nicht mehr angezeigt.

Tastaturbefehle auf dieser Seite

- Alt + q = Button "Quellverzeichnis nutzen"

- Alt + z = Button "Zielverzeichnis wählen"

6.7.4 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. Wenn Sie mit der Maus auf diesen Status zeigen, wird in einem Tooltip die Fehlerursache angezeigt.
- **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.
-  : Über dieses Symbol wird die unter "Ergebnisdatei" aufgeführte Datei angezeigt.

Dateien mit folgendem Programm weiterverarbeiten

Benutzen Sie die Auswahlliste um ein Programm auszuwählen, mit dem die entschlüsselten Dateien weiterverarbeitet werden sollen. Die Voreinstellung ist "Keine Weiterverarbeitung". Das ausgewählte Programm wird direkt mit den signierten Dateien aufgerufen. Die Auswahlliste zeigt alle Programme an, die Sie im Dialog "Einstellungen" in der Registerkarte "Anwendungen" konfiguriert haben, siehe Kapitel 5.2.

Bitte beachten Sie, dass bei einem macOS nur die Standardfunktionen zur Verfügung stehen. Die Übergabe von Dateien an Programme, die in "Anwendungen verwalten" angegeben wurden, funktioniert bei einem macOS nicht.

Ergebnisdatei vorhanden

Wenn beim Erstellen der Ergebnisdatei bemerkt wird, dass eine Datei mit gleichem Namen im Zielverzeichnis bereits vorhanden ist, wird der Dialog "Datei vorhanden" angezeigt. Sie haben

hier die Möglichkeit, eine Auswahl zu treffen. Sie können die Datei überschreiben oder umbenennen lassen. Beim Umbenennen wird der Datei das aktuelle Datum im Dateinamen vorangestellt. Sie können die Verarbeitung aber auch abbrechen.

Hinweis: Sie können Weiterverarbeitung auch noch **nach** der Verarbeitung der Dateien auswählen. Klicken Sie dann nach der Auswahl des Nachfolgeprogramms auf das ▶ Symbol, um die Ausführung zu starten. **Achtung**: Es werden **alle** Ergebnisdateien an das Nachfolgeprogramm übergeben.

Letzte Dialogseite der Funktion Entschlüsseln

Auf der letzten Dialogseite der Funktion Entschlüsseln wird unterhalb der Dateiliste die Auswahl des Nachfolgeprogramms angezeigt. Klicken Sie auf den Entschlüsseln-Button, um den Prozess zu starten.

Passwort-basierte Entschlüsselung

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

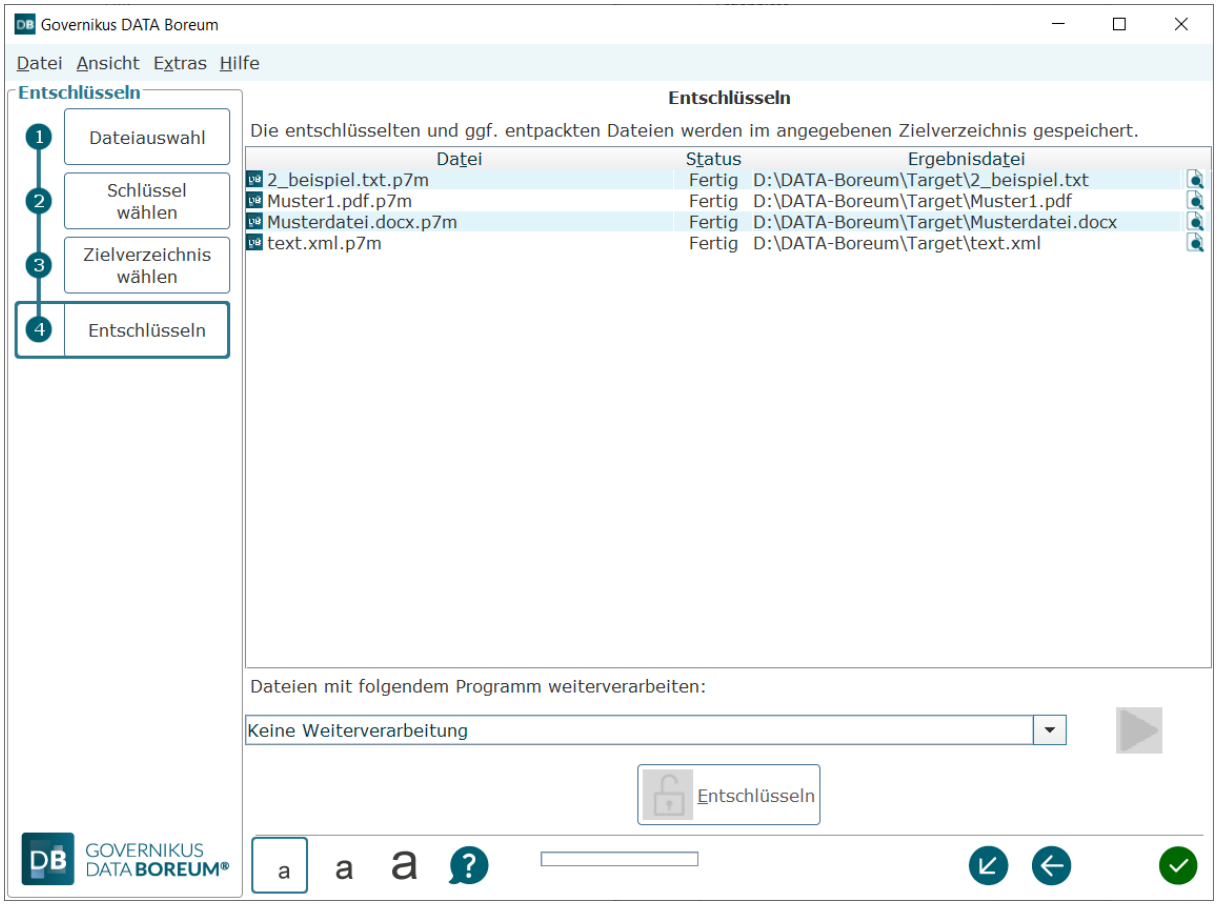

Abbildung 45: Letzte Dialogseite der Funktion Entschlüsseln

Tastaturbefehle auf dieser Seite

- Alt + t = Fokus in die Tabelle setzen
- Alt + Enter = Button "Entschlüsseln"

7 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 **Fehler! Verweisquelle konnte nicht gefunden werden.**.
- **DATA Boreum als Hintergrundprozess**: DATA Boreum lässt sich als Hintergrundprozess starten. Damit sind die kryptografischen Funktionen schneller aufrufbar, siehe Kapitel 7.2.

7.1 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 ist im Kapitel Einstellungen in der Registerkarte „Governikus“ erklärt, siehe Kapitel 5.4.

7.2 Governikus DATA Boreum als Hintergrundprozess

Governikus DATA Boreum lässt sich als Hintergrundprozess starten, mit dem Effekt, dass die die kryptografischen Funktionen schneller aufrufbar sind.

Governikus DATA Boreum als Hintergrundprozess für Linux

Für Linux steht Governikus DATA Boreum als Hintergrundprozess nicht zur Verfügung.

Governikus DATA Boreum als Hintergrundprozess für macOS

Für macOS steht Governikus DATA Boreum als Hintergrundprozess zur Verfügung. Governikus DATA Boreum wird für macOS als ZIP-Datei ausgeliefert. Diese ZIP-Datei enthält diese beiden Apps:

- `DATABoreumOffline.app`: Benutzen Sie diese App, um Governikus DATA Boreum, wie gewohnt, als Programm im Vordergrund starten.
- `DATABoreumServiceOffline.app`: Benutzen Sie diese App um Governikus DATA Boreum als Hintergrundprozess zu betreiben.

Installieren Sie die App `DATABoreumServiceOffline` wie gewohnt, und fügen Sie die App für den Schnellzugriff dem Dock hinzu. Sie können jetzt mit einem Rechtsklick das Kontextmenü aufrufen. Die Funktionen des Kontextmenüs sind identisch mit denen, die im folgenden "Abschnitt Governikus DATA Boreum als Hintergrundprozess für Windows" erklärt werden.

Governikus DATA Boreum als Hintergrundprozess für Windows

Bei Windows gibt es nach der Installation von Governikus DATA Boreum einen weiteren Eintrag im Startmenü mit dem Titel " Governikus DATA Boreum Service". Haben Sie die Offline-Variante installiert, steht hinter dem Eintrag zusätzlich die Bezeichnung "Offline".

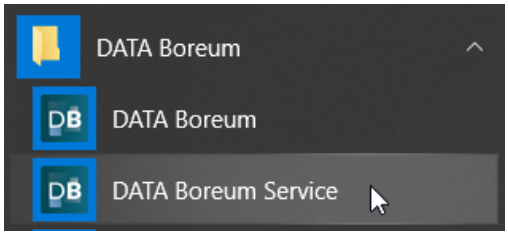

Abbildung 46: Zusätzlicher Eintrag im Startmenü

Starten von Governikus DATA Boreum als Hintergrundprozess

Wenn Sie den Eintrag "Governikus DATA Boreum Service" auswählen, wird Governikus DATA Boreum gestartet und ist dann über den Windows-Infobereich (Tray) erreichbar. Mit einem Rechtsklick auf das Governikus DATA Boreum-Symbol erreichen Sie das Kontextmenü.

	**Hinweis**: Das Umschalten zwischen der Deutschen und Englischen Benutzeroberfläche ist nur in der Variante möglich, die im Vordergrund ausgeführt wird. Rufen Sie diese Version auf, ändern Sie hier die Spracheinstellung, schließen Sie diese Version und rufen Sie dann wieder Governikus DATA Boreum als Hintergrundprozess auf.

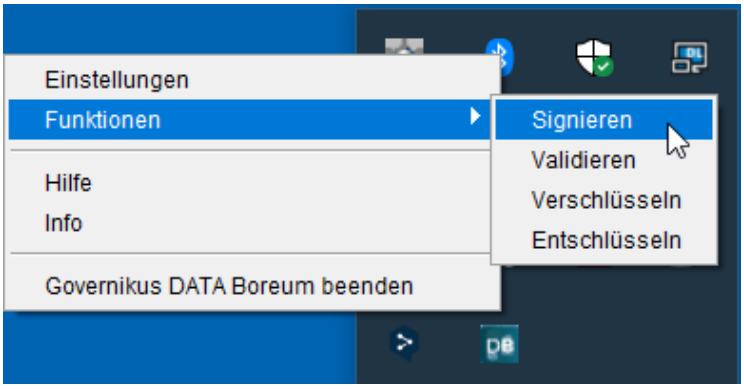

Abbildung 47: Kontextmenü von Governikus DATA Boreum im Tray

	Hinweis für macOS: Bei macOS sind dieselben Einträge vorhanden. Das Layout ist ähnlich im Mac OS Design.

Die folgenden Einträge sind über das Kontextmenü erreichbar:

- **Einstellungen**: Diese Option öffnet den Einstellungsdialog, dieser ist im Kapitel 5 erklärt.
- **Funktionen**: Im Eintrag "Funktionen" können Sie die kryptografischen Funktionen Signieren, Validieren, Verschlüsseln und Entschlüsseln auswählen. Diese sind in den Kapiteln 6.4 bis 6.7erklärt.
- **Hilfe**: Der Eintrag "Hilfe" ruft die Online-Hilfe von Governikus DATA Boreum auf.
- **Info**: Der Eintrag "Info" ruft das Dialogfenster mit den Informationen zu Governikus DATA Boreum Version, Lizenz und weiteren Einträgen auf. Klicken Sie auf das Dialogfenster, um es zu schließen.
- **Governikus DATA Boreum beenden**: Mit diesem Eintrag wird Governikus DATA Boreum beendet. Das Symbol im Tray wird nicht mehr angezeigt.

	Hinweis: Wird Governikus DATA Boreum als Hintergrundprozess betrieben, wird der Arbeitsspeicher nur mit ca. 140 MB belastet, da die GUI erst beim Aufruf gestartet wird.

Governikus DATA Boreum als Hintergrundprozess beim Start des Computers

Sie können Governikus DATA Boreum als Hintergrundprozess beim Start des Computers starten. Kopieren Sie dazu einfach den Eintrag " Governikus DATA Boreum Service" im Windows Startmenü in das Verzeichnis "Autostart" im Windows Startmenü.

Aufruf der kryptographischen Funktionen im Explorer

Dem Kontextmenü des Explorers wurden bei der Installation von Governikus DATA Boreum die Aufrufe der kryptografischen Funktionen hinzugefügt, die im Kapitel 6.3.2 erklärt sind. Ist Governikus DATA Boreum bereits als Hintergrundprozess gestartet, ist der Aufruf einer kryptografischen Funktion deutlich schneller. Ist Governikus DATA Boreum noch nicht gestartet, dauert dieser Aufruf deutlich länger.

8 Besonderheiten der Integration Edition

Die Governikus DATA Boreum Integration Edition wird von einer Fachanwendung direkt über einen Webservice (SOAP), die Java-API oder per Kommandozeile aufgerufen. Dabei werden mit dem Aufruf Dateien zur Weiterverarbeitung an die Funktionen von Governikus DATA Boreum übergeben.

Hinweis: Bitte beachten Sie, dass Governikus DATA Boreum in der Integration Edition keinen Eintrag im Startmenü besitzt, da er durch eine Fachanwendung aufgerufen wird und sich nach der Verarbeitung der übergebenen Dateien automatisch schließt.

Die Governikus DATA Boreum Integration Edition kann ausschließlich als Hintergrundanwendung gestartet werden und ist über ein Icon im Systemdienst sichtbar, siehe auch Kapitel 8.3. Die Benutzeroberfläche öffnet sich nur bei einem Aufruf durch eine Fachanwendung.

Neben der Installationsdatei ist die Governikus DATA Boreum Integration Edition auch in einer Portable-Variante verfügbar, die nicht über ein Installationsprogramm installiert wird. Diese Variante steht in Form eines ZIP-Archivs bereit, welches an die gewünschte Stelle extrahiert werden muss. Anschließend ist die Governikus DATA Boreum Integration Edition direkt von dort aus startbar. Die Governikus DATA Boreum Integration Edition kann auf diesen Betriebssystemen betrieben werden:

- Windows ,
- Linux und
- macOS .

8.1 Konfiguration

Ihr Diensteanbieter stellt die Governikus DATA Boreum Integration Edition bereit. Er hat die Möglichkeit, dieses Programm vielfältig anzupassen, so dass es genau auf die Bedürfnisse und Anforderungen der vorliegenden Fachanwendung eingestellt ist.

Ausgegraute oder ausgeblendete Dialogseiten

Jede der Funktionen Signieren, Validieren sowie Ver- und Entschlüsseln besteht aus mehreren Dialogseiten. Die jeweils letzte Dialogseite ist immer verfügbar. Weitere Dialogseiten können teilweise ausgegraut oder ganz ausgeblendet sein. In diesem Fall können Sie auf dieser Seite nur wenige oder keine Einstellungen vornehmen und sich nur über die festgelegten Einstellungen informieren. Sind einzelne Einstellungsmöglichkeiten oder ganze Dialogseiten ausgeblendet, hat Ihr Diensteanbieter die dort möglichen Einstellungen bereits fest eingestellt und bietet den Dialog nicht mehr an. Auch Menüeinträge bzw. die gesamte Menüzeile können ausgeblendet werden.

Konfigurationsdatei

Typischerweise werden die zur Anwendung der Governikus DATA Boreum Integration Edition notwendigen Einstellungen durch Ihren Diensteanbieter vorgegeben. Ihr Diensteanbieter kann es Ihnen aber auch ermöglichen, selbst Einstellungen vorzunehmen und dauerhaft in einer Konfigurationsdatei zu speichern, siehe dazu Kapitel 8.2. Es werden dabei alle aktuellen Einstellungen aus den Dialogschritten und dem Einstellungsdialog gespeichert. Diese

gespeicherten Einstellungen werden dann mit jedem Aufruf der Governikus DATA Boreum Integration Edition verwendet. Beachten Sie, dass Ihr Diensteanbieter mit jedem Aufruf der Governikus DATA Boreum Integration Edition die Möglichkeit hat, andere Einstellungen vorzugeben. Diese Vorgaben gelten für einen konkreten Aufruf und werden nicht automatisch gespeichert.

8.2 Menüleiste der Integration Edition

Die Menüleiste der DATA Boreum Integration Edition unterscheidet sich von DATA Boreum in den Optionen des Menüs "Extras".

Extras -> Einstellungen

Die Option "Einstellungen" öffnet das Dialogfenster "Einstellungen". Im Gegensatz zu DATA Boreum können Sie in der Integration Edition Ihre Änderungen hier nicht dauerhaft speichern, sondern nur vorübergehend übernehmen. Das bedeutet, dass diese von Ihnen geänderten Einstellungen nur für die Dauer dieses Aufrufs bestehen. Nach der Verarbeitung der übergebenen Dateien und dem automatischen Schließen der Anwendung danach, werden die Änderungen verworfen.

Extras -> Einstellungen dauerhaft speichern

Wenn Sie im Dialogfenster "Einstellungen" oder auf anderen Dialogseiten von Governikus DATA Boreum Änderungen vorgenommen haben, die Sie dauerhaft speichern wollen, benutzen Sie diese Option. Damit werden alle Änderungen in der Konfigurationsdatei dauerhaft gespeichert. Bereits zuvor in der Konfigurationsdatei gespeicherte Einstellungen werden überschrieben. Wenn Sie die "alten" Einstellungen vorher sichern wollen, lesen Sie bitte den folgenden Absatz "Einstellungen exportieren".

Extras -> Einstellungen exportieren

Benutzen Sie diese Option, um die Konfigurationsdatei, die die Einstellungen von Governikus DATA Boreum enthält, zu exportieren. Bitte beachten Sie dabei, dass die Datei die Endung `xml` haben muss. Vergeben Sie einen erklärenden Namen für die Konfigurationsdatei. Exportieren Sie beispielsweise die Konfigurationsdatei mit den Grundeinstellungen, die mit der Installation vorliegen, nennen Sie die Datei beispielsweise `Basis-Konfiguration.xml`. Wenn Sie beispielsweise die Einstellungen über das Dialogfenster "Einstellungen" geändert haben oder über die Dialogseiten von Governikus DATA Boreum, damit diese für eine bestimmte, aufrufende Fachanwendung XYZ passen, dann speichern Sie diese dauerhaft, siehe Absatz oben "Extras -> Einstellungen dauerhaft speichern". Exportieren Sie danach die Einstellungen und nennen Sie die Konfigurationsdatei beispielsweise `XYZ-Konfiguration.xml`. Beachten Sie beim dauerhaften Speichern, dass Sie bereits vorhandene Einstellungen überschreiben. Exportieren Sie gegebenenfalls "alte" Einstellungen, bevor Sie die neuen Einstellungen dauerhaft speichern.

Mit dem Exportieren von Konfigurationsdateien, die bestimmte Einstellungen für bestimmte Fachanwendungen enthalten, können Sie erreichen, dass Sie diese Einstellungen immer wieder benutzen können. Vor dem Aufruf von Governikus DATA Boreum mit der Fachanwendung XYZ können Sie die dazu passende Konfigurationsdatei `XYZ-Konfiguration.xml` importieren und damit sicherstellen, dass die Funktionen von DATA Boreum mit den korrekt angepassten Einstellungen durchgeführt werden. Das Importieren von Konfigurationsdateien können Sie über die entsprechende Option des Tray-Icons durchführen, siehe nächstes Kapitel "Optionen über das Tray-Icon aufrufen".

8.3 Optionen über das Tray-Icon aufrufen

Governikus DATA Boreum bietet über das Tray-Icon weitere Optionen an. Sie erreichen diese Optionen, wenn Sie den Mauszeiger auf das Governikus DATA Boreum Symbol im Tray legen (üblicherweise rechts unten auf dem Desktop) und mit der rechten Maustaste das Kontextmenü aufrufen, siehe nächste Abbildung.

Abbildung 48: Optionen des Governikus DATA Boreum Tray-Icons

Einstellungen importieren

Wenn Sie diese Optionen wählen, können Sie eine Konfigurationsdatei für Governikus DATA Boreum importieren. Bitte beachten Sie, dass Sie diesen Import vor dem Aufruf von Governikus DATA Boreum durchführen müssen. Ist die Benutzeroberfläche von Governikus DATA Boreum bereits gestartet, führt der Aufruf "Einstellungen importieren" zu einer Fehlermeldung. Wenn Sie die Option "Einstellungen importieren" ausgewählt haben, wird ein Dialogfenster zur Dateiauswahl geöffnet. Wechseln Sie in das Verzeichnis, das Ihre Governikus DATA Boreum Konfigurationsdateien enthält und wählen Sie die Datei aus, die Sie als nächste benötigen.

Info

Wenn Sie diese Option auswählen, wird dasselbe Dialogfenster geöffnet, das auch in Governikus DATA Boreum über das Menü "Hilfe" und die Option "Über Governikus DATA Boreum" angezeigt wird. Es enthält Versionsinformationen. Klicken Sie auf das Dialogfenster, um es zu schließen.

Governikus DATA Boreum beenden

Wenn Sie diese Option auswählen, wird Governikus DATA Boreum beendet. Mit dieser Option wird das Tray-Icon entfernt und die Anwendung vollständig geschlossen. Bitte beachten Sie, dass auch die Benutzeroberfläche von Governikus DATA Boreum mit dieser Option geschlossen wird, wenn sie zuvor geöffnet war.

Um Governikus DATA Boreum zu beenden, klicken Sie einmal auf das Tray Icon um es zu aktivieren, gefolgt von einem Doppelklick, um das Programm zu beenden.

8.4 Die Funktionen der Integration Edition

Signieren, Validieren, Verschlüsseln, Entschlüsseln

Obwohl Governikus DATA Boreum in der Integration Edition über alle Funktionen von DATA Boreum verfügt, werden die Funktionen durch die aufrufende Fachanwendung vorgegeben. Wenn eine Fachanwendung die Integration Edition beispielsweise mit der Funktion "Signieren" aufruft, ist es nicht möglich, zu einer anderen Funktion zu wechseln.

Zeitstempel

Wenn die Integration Edition mit der Funktion "Signieren" aufgerufen wird, steht auch die Möglichkeit zur Verfügung, einen Zeitstempel anzubringen - es sei denn, der Diensteanbieter hat diese Option ausgeblendet.

9 Erläuterungen

Im Folgenden werden die Begriffe und Hintergründe erläutert, die im Kontext von Governikus DATA Boreum wichtig sind. Mit den Erläuterungen soll das Verständnis der zur Verfügung gestellten Funktionalitäten vertieft werden. 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 von Governikus DATA Boreum keine immer zutreffende, logische Reihenfolge geben kann.

9.1 Authentifizierung und Authentisierung

Diese beiden Begriffe bedeuten im Deutschen tatsächlich 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.

9.2 Entschlüsselung

Die Entschlüsselung wird angewendet, wenn eine Datei zuvor verschlüsselt wurde. Das Kapitel 9.8 "Verschlüsselung" erklärt Ver- und Entschlüsselung.

9.3 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. Bei elektronischen Signaturen werden die folgenden Typen unterschieden, von denen nur die letzte rechtlich einer eigenhändigen Unterschrift weitestgehend gleichgestellt ist.

- 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)

Authentizität und Integrität

Ziel der elektronischen Signatur ist es, die Authentizität und Integrität von Daten nachzuweisen. 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, das Zertifikat des Schlüssels (Signaturkarte oder Keystore) ausgewählt, mit dem die Signatur erstellt werden soll. Dieses Zertifikat wird der Datei hinzugefügt. Über den Inhalt der Datei samt Zertifikat wird ein Hashwert errechnet, im zweiten Schritt wird der Hashwert mit dem privaten Schlüssel verschlüsselt und im dritten wird der verschlüsselte Hashwert dem Dokument hinzugefügt, wodurch die Signatur entsteht.

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, der mit dem Secure Hashing Algorithm (SHA) mit 256 Zeichen Schlüssellänge erstellt wurde. Hashwerte, die mit SHA256 errechnet werden, haben im 64 alphanumerische Zeichen:

```
0D9C3ECDFBE036E1750DE82A7863F1E6B6AC336B
```

Ein Hashwert ist für jede Datei einmalig. Wenn für eine Datei immer dieselbe Hash-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. Bei der Integritätsprüfung wird der Hashwert für die Datei neu berechnet und mit dem verschlüsselten Hashwert der Signatur verglichen. Sind beide Hashwerte gleich, wurde die Datei nicht verändert. Diese Integritätsprüfung wird auch mathematische Prüfung genannt.

2. Verschlüsselung des Hashwerts

Für die Verschlüsselung des Hashwerts wird ein so genanntes asymmetrisches Schlüsselpaar benutzt. Es besteht aus einem privaten (geheimen) und einem öffentlichen Schlüssel. Der private Schlüssel ist nur auf der Signaturkarte oder im Keystore 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 Governikus DATA Boreum, 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.

Signierte Datei

Die oben erklärten Bestandteile - verschlüsselter Hashwert, Verschlüsselungszeitpunkt und Zertifikat mit öffentlichem Schlüssel - sind 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 eigenen, gesonderten Datei enthalten, dann heißt die Signatur "detached". Das Zertifikat kann bis zur qualifizierten Vertrauensdiensteanbieter (qVDA), der das Zertifikat herausgegeben hat, nachvollzogen werden. Der qVDA 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.

9.4 Signaturalgorithmus

Ein Signaturalgorithmus ist ein Verschlüsselungsverfahren, das bei der Erstellung von elektronischen Signaturen verwendet wird. Ein Signaturalgorithmus verschlüsselt immer den Hashwert, siehe Abschnitt "Wie entsteht eine qualifizierte elektronische Signatur?" im Kapitel 9.3.

In den Empfehlungen der SOG-IS zum Algorithmenkatalog werden alle Algorithmen gelistet, die für die Erzeugung eines Hashwerts und für die Verschlüsselung bei der Erzeugung der elektronischen Signatur geeignet sind.

Bezugsquellen: Hier finden Sie die Seite der SOG-IS zum Thema empfohlene Krypto-Algorithmen und Algorithmenkatalog

Bitte beachten Sie, dass die Verschlüsselung des Hashwerts mit einem Signaturalgorithmus nicht zu einem Schutz der Inhaltsdaten führt. Die signierte Datei enthält unter anderem den öffentlichen Schlüssel, der zur Entschlüsselung der Signatur benutzt werden muss, damit die Signatur geprüft werden kann. Die Verschlüsselung zum Schutz von Inhaltsdaten ist in Kapitel 9.8 erklärt.

9.5 Signaturformate

Formate elektronischer Signaturen

Eine Signatur, siehe Kapitel 9.3, kann in verschiedenen Formaten vorliegen. Governikus DATA Boreum unterstützt verschiedene elektronische Signaturformate. Diese Formate sind international standardisierte Signatur- und Dateiformate. Die unterstützen Formate sind:

CAdES

CAdES ist das Akronym für CMS Advanced Electronic Signatures. Ein Vorteil dieser Erweiterung von CMS ist, dass die Gültigkeit von Dokumenten, die so signiert werden, vergleichsweise lang ist, unabhängig von verwendeten Verschlüsselungs-algorithmen. Das Hauptdokument für die Beschreibung dieses Formats befindet sich in ETSI TS 101 733 des European Telecommunications Standards Institute. CAdES entspricht den Anforderungen der EU an elektronische Signaturen.

PDF mit eingebetteten CAdES-Signaturen

Dieses Format ist eine Variante des oben beschriebenen CAdES-Formats. Dabei bleibt die PDF-Datei weiter durch jeden beliebigen PDF-Reader anzeigbar, da die Signaturen in einer eigenen Registerkarte des PDF-Readers aufgeführt werden.

Spezielle PDF-Signaturformate

Es stehen PDF- und CAdES-Signaturformate zur Verfügung.

- **PDF**: Es werden zwei Methoden für PDF-Signaturen unterstützt:
  - **PAdES**: Dieses Akronym 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 dem Signaturformat PDF-Inline entsprechen. PAdES geht über das einfache Signaturformat PDF-Inline hinaus und ermöglicht die zukunftssichere Validierung von signierten PDF-Dokumenten. PAdES entspricht den Anforderungen der EU an elektronische Signaturen.
  - **PDF-Inline**: Dieses Signaturformat ist in den Normen ISO 32000 und ISO 19905 definiert und ist in nahezu allen PDF-Softwareprodukten implementiert.

Associated Signature Containers (ASiC)

Das European Telecommunications Standards Institute (ETSI) hat einen Europäischen Standard für eine signierte Container-Struktur (ASiC) herausgegeben. Als Container-Struktur wird das ZIP-Dateiformat benutzt. Die Signaturformate sind CAdES oder XAdES. ASiC bietet damit Möglichkeit die sonst typische Trennung bei detached Signaturen zu umgehen und die Dokumente im Container zu kapseln. Dies spielt vor allem bei den XAdES Signaturen eine Rolle, da diese eine beliebige Anzahl von Dateien durch eine einzige XAdES Signatur signieren können. Optional können auch Zeitstempel enthalten sein. Signierte Associated-Signature-Container-Dateien haben die Dateiendung `scs` oder `asics`.

9.6 Signaturkarte

Eine Signaturkarte hat üblicherweise das Format einer Scheckkarte und enthält einen Chip. Dieser Chip enthält Zertifikate.

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 und die Schlüsselverwendung.

9.7 Validieren

Das Validieren ist ein Vorgang, bei dem eine elektronisch signierte Datei auf Authentizität und Integrität überprüft wird. Mit dem öffentlichen Schlüssel, der im mitgelieferten Zertifikat der elektronischen Signatur enthalten ist, kann der Hashwert entschlüsselt werden. Nach der Neuberechnung des Hashwerts kann dieser mit dem entschlüsselten Hashwert verglichen werden. Sind diese gleich, ist die Integrität des signierten Dokuments nachgewiesen. Zum Nachweis der Authentizität, also der Identität desjenigen, der behauptet, die Datei signiert zu haben, wird das Zertifikat zur Online-Prüfung an den herausgebenden qualifizierten Vertrauensdiensteanbieter (qVDA) geschickt. Dazu muss in den Einstellungen von Governikus DATA Boreum (siehe Kapitel 5 "Einstellungen") ein Validierungsdienst konfiguriert werden. Über diesen und weitere Dienste wird über gesicherte Kommunikation das Zertifikat bis zum qVDA weitergereicht.

Zertifikatsprüfung

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

9.8 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 (siehe Kapitel 9.2). 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 von Governikus DATA Boreum 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 Governikus DATA Boreum dazu 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 verschlüsselt, hinzugefügt. Als Benutzer merken Sie von diesem zweistufigen Verfahren nichts.

Hinweis: Für die Verschlüsselung benutzt DATA Boreum immer die Ciphersuite AES-256-GCM.

Das BSI (siehe technische Richtlinie BSI TR-3116-4) und die IETF (siehe RFC 7525) empfehlen AES-256-GCM für die symmetrische Verschlüsselung und SHA256 als Digest Algorithmus und stufen diese Ciphersuite als sicher ein.

9.9 Zeitstempel

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

Abhilfe schafft ein externer Zeitstempel von einer vertrauenswürdigen Stelle oder, wenn Rechtsgültigkeit erforderlich ist, ein qualifizierter elektronischer Zeitstempel von einem akkreditierten Zeitstempeldienstanbieter. Dieser qualifizierte elektronische Zeitstempel wird in die Signatur eingebettet und bietet eine vertrauenswürdige und beweiswerte Zeitangabe. Die Aussage des Zeitstempels ist: Der Zeitstempeldienst hat bestätigt, dass die Signaturdatei zu dem angegebenen Zeitpunkt existiert hat. Ein Zeitstempel eines zertifizierten Zeitstempeldienstes hat seinerseits eine digitale Signatur, die ebenfalls validierbar ist.

9.10 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.

10 Sicherheit und Datenschutz

Governikus DATA Boreum ist eine sichere Anwendung für kryptografische Anwendungen. 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 von Governikus DATA Boreum werden besondere Anforderungen an die Software und die Einsatzumgebung gestellt. Dies Anforderungen sind als Empfehlungen formuliert und werden im folgenden Kapitel beschriebe.
- **Privacy by Design**: Bei der Erhebung und Verarbeitung personenbezogener Daten ist durch §3a des Bundesdatenschutzgesetzes Datenvermeidung und Datensparsamkeit vorgegeben. Wie die Governikus KG dies umsetzt ist im Kapitel 10.2 beschrieben.
- **Security by Design**: Die Governikus KG hat Mechanismen etabliert, um die höchstmögliche Sicherheit ihrer Software zu garantieren. Dies ist in Kapitel 10.3 beschrieben.

10.1 Empfehlungen für den Betrieb

Um qualifizierte elektronische Signaturen und Siegel sicher, korrekt und vertrauenswürdig anbringen und prüfen 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. sie wird immer durch einen "Mix" von Sicherheitsvorkehrungen in der Software selbst und in der Einsatzumgebung komplettiert.

10.1.1 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 Governikus DATA Boreum betrieben wird, dürfen keine Angriffe ausgehen. Installierte Software darf nicht böswillig manipuliert oder verändert werden. Maßnahmen gegen Viren oder trojanische Pferde 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 Governikus DATA Boreum 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.

10.1.2 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 Benutzenden, die Governikus DATA Boreum betreiben, 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, siehe Kapitel 3.

10.1.3 Technische Anforderungen

Die von Governikus DATA Boreum unterstützte Hard- und Software ist im Handbuch "Governikus DATA Boreum - Systemanforderungen" beschrieben. Zur Ausstattung für die Erstellung von qualifizierten elektronischen Signaturen und Siegeln zählen die folgenden Karten und Chipkartenleser:

- Es können qualifizierte elektronische Signaturerstellungseinheiten sowie qualifizierte 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.

10.1.4 Anforderungen an die Konfiguration

Hinsichtlich der Konfiguration müssen Sie folgende Anforderungen berücksichtigen:

- **Validierungsdienst**: Um die Gültigkeit von qualifizierten elektronischen Signaturen prüfen zu können, ist ein vertrauenswürdiger Validierungsdienst einzurichten (vgl. Kapitel 5.7). Die Verbindungsdaten sowie das erforderliche Zertifikat erhalten Sie über Ihren Governikus Suite Administrator.
- **Zeitstempeldienst**: Für das Anbringen von qualifizierte Zeitstempeln ist ein vertrauenswürdiger Zeitstempeldiensteanbieter einzurichten (vgl. Kapitel 5.4), der die qualifizierten Zeitstempel über diesen Zeitstempeldiensteanbieter erstellen lässt. Die Verbindungsdaten erhalten Sie über Ihren Governikus Suite Administrator.

10.2 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.

10.2.1 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.

10.2.2 Privacy by Default - Produktkonfiguration

Governikus DATA Boreum signiert, validiert, ver- und entschlüsselt Dokumente. Bei der Verarbeitung von Dateien (Signieren, Validieren, Verschlüsseln und Entschlüsseln) werden nach dem Beenden der Verarbeitung keine Daten in der Software gespeichert.

Die Konfiguration von Governikus DATA Boreum 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.

	**Hinweis**: Bei der Validierung von Signaturen und der Validierung von Zertifikaten werden Prüfprotokolle erstellt. Diese Prüfprotokolle enthalten persönliche Daten (Name des Zertifikatsinhabers und Name der Zertifizierungsstelle), die aus den Zertifikaten ausgelesen werden. Die Prüfprotokolle werden als Datei in dem Verzeichnis gespeichert, dass Sie als Zielverzeichnis angelegt haben. Bitte achten Sie darauf, dass dieses Verzeichnis vor dem Zugriff Dritter geschützt ist. Löschen Sie die Prüfprotokolldateien, wenn Sie nicht mehr benötigt werden.

10.3 Security by Design

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

10.3.1 Überwachung von Drittanbieter-Produkten

In Governikus DATA Boreum sind auch Programme von Drittanbietern enthalten, sogenannte 3rd Party Libs. Die in Governikus DATA Boreum enthaltenen Programme von Drittanbietern werden im Dokument " Governikus DATA Boreum 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.

10.3.2 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.

10.3.3 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.

10.4 DSGVO und Governikus DATA Boreum

Einleitung

Die DSGVO regelt den Schutz personenbezogener Daten und die Rechte der Bürger an ihren personenbezogenen Daten. Die Governikus KG liefert mit ihrem Produkt Governikus DATA Boreum eine Software aus, die zum Teil auch personenbezogene Daten verarbeitet. Die folgende Beschreibung liefert die entsprechenden Aussagen zu den Funktionen von Governikus DATA Boreum.

Download und Installation

Beim Download von Governikus DATA Boreum ist die Kommunikation zwischen dem Rechner des Benutzers und dem Download-Server der Governikus KG SSL-verschlüsselt. Die IP-Adresse des Benutzers wird auf dem Download-Server im Server-Protokoll anonymisiert gespeichert, indem die letzten beiden der vier IP-Blöcke jeweils den Wert 0 erhalten. Damit ist eine Rückverfolgung des Benutzers nicht mehr möglich.

In den Installations- und Programmpaketen von Governikus DATA Boreum sind keine personenbezogenen Daten enthalten, weder bei der Online-Version (Programmdaten werden beim Aufruf von Governikus DATA Boreum auf Aktualität geprüft und gegebenenfalls nachgeladen) noch bei der Offline-Version (Programmdaten werden beim Aufruf ohne Prüfung auf Aktualität direkt geladen).

Zertifikate mit personenbezogenen Daten

Für das Signieren von Dateien, für die Validierung von Zertifikaten und für die Validierung von Signaturen 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.

Die Verwendung von Zertifikaten, die auf Personen ausgestellt sind, ist für die Erstellung von qualifizierten elektronischen Signaturen notwendig. Ohne diese Daten kann die Funktion Signieren nicht durchgeführt werden. Das Einverständnis des Betroffenen bei der Verarbeitung dieser personenbezogenen Daten, die der Betroffene in seinen Zertifikaten hat eintragen lassen, wird also implizit vorausgesetzt, da sonst das Signieren nicht möglich ist. Die Verantwortung für das datenschutzkonforme Ausstellen und Veröffentlichen von Zertifikaten liegt bei der Zertifizierungsstelle, also dem Zertifizierungsdienstanbieter.

Konfiguration von Governikus DATA Boreum

Die Konfiguration von Governikus DATA Boreum wird in einer XML-Datei gespeichert. Diese wird als Standardeinstellung im Profil-Ordner des Benutzers gespeichert, der Speicherort kann vom Benutzer verändert werden:

- **Windows**: Der Profil-Ordner liegt im Verzeichnis `C:\Users\<Benutzername>`
- **Linux**: Der Profil-Ordner liegt im Verzeichnis `/home/<Benutzername>`

Die Konfigurationsdatei heißt `data_boreum.xml`. Außer zwei möglichen Ausnahmen enthält die Konfigurationsdatei keine personenbezogenen Daten.

- **Validieren**: Zum Validieren muss eine Verbindung zum Validierungsdienst konfiguriert werden. Der Validierungsdienst signiert die Antworten mit dem Prüfergebnis. Damit diese Signatur von Governikus DATA Boreum geprüft werden kann, muss das Signaturzertifikat des Validierungsdienstes in der Konfiguration hinterlegt werden. Üblicherweise kommt hier ein Signaturzertifikat aus einer internen PKI zum Einsatz. Es kann auch ein Signaturzertifikat eingesetzt werde, dass personenbezogenen Daten enthält.

Log-Dateien

In den Log-Dateien von Governikus DATA Boreum sind keine personenbezogenen Daten enthalten. Weder beim Signieren noch beim Validieren werden Zertifikatsdaten in der Log-Datei protokolliert.

Prüfprotokoll

Das Prüfprotokoll beschreibt das Ergebnis der Validierung eines Zertifikats, respektive der Validierung einer Signatur. Es enthält die personenbezogenen Daten aus dem jeweiligen Zertifikat. Ohne diese Daten kann keine Prüfung vorgenommen werden. Das Prüfprotokoll wird in demselben Verzeichnis gespeichert, in dem die Datei liegt, deren Zertifikat, respektive deren Signatur geprüft wurde. Es findet keine automatische Löschung der Prüfprotokolle statt. Es liegt in der Verantwortung des Benutzers von Governikus DATA Boreum, Prüfprotokolle in einer geschützten Umgebung zu speichern und diese zu löschen, wenn die Aufbewahrung nicht mehr notwendig ist.

Datensparsamkeit

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

Schutz der Daten vor unbefugtem Zugriff durch Dritte

Der Ort der Speicherung von Zertifikatsdaten, Prüfprotokollen und signierte Dateien liegt in der Verantwortung des Benutzers von Governikus DATA Boreum. Folgt der Benutzer den Empfehlungen für den Betrieb, die im Kapitel 10.1 beschreiben sind, ist ein angemessener Schutz gewährleistet. Die Umsetzung der Empfehlungen liegt in der Verantwortung des Benutzers und ist dem Einfluss der Governikus KG entzogen.

10.5 Gesetzliche Grundlagen

EU DS GVO

Die EU-Datenschutz-Grundverordnung (EU DS GVO) 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.

11 Erste Hilfe

In diesem Kapitel finden Sie Hinweise und Lösungsmöglichkeiten für den Fall, dass es bei der Verwendung von Governikus DATA Boreum zu Problemen kommen sollte. Die Hinweise gelten für alle Editionen.

Signaturkarte kann nicht ausgewählt werden

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

Ein neu angeschlossener Chipkartenleser steht nicht zur Auswahl

- Symptom:
  - Ein Chipkartenleser wurde angeschlossen. Er wird jedoch nicht unter "Speicherort des Schlüssels" aufgelistet.
- Mögliche Ursache:
  - Governikus DATA Boreum prüft nur beim Programmstart, welche Chipkartenleser verfügbar sind. Nachträglich angeschlossene Chipkartenleser werden nicht automatisch erkannt. Bitte führen Sie in diesem Fall die Funktion "Karten neu einlesen" aus.
  - Der Chipkartenleser wird durch Governikus DATA Boreum nicht unterstützt. Prüfen Sie bitte anhand des beiliegenden Dokumentes "Systemanforderungen", ob Ihr Chipkartenleser unterstützt wird.
  - Die Treiber-Software für den Chipkartenleser 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.

Keine bzw. nicht alle Dateien zur Validierung auswählbar

- Symptom:
  - Nach Aufruf der Funktion "Dateien hinzufügen" für die Validierung werden im Dialogfenster zur Dateiauswahl keine bzw. nicht alle der tatsächlich im gewählten Verzeichnis vorhandenen Dateien angezeigt.
- Ursache:
  - Governikus DATA Boreum zeigt in diesem Dateiauswahldialog nur potentiell validierbare Dateien an, die den unterstützten Signaturformaten entsprechen. Das sind z.B. CAdES-Signaturdateien sowie Dateien, die eine Signatur enthalten könnten, z.B. PDF-Dateien. Die Prüfung erfolgt dabei anhand des Dateiinhalts und nicht der

Dateiendung und kann je nach Anzahl der Dateien in dem gewählten Verzeichnis einen kleinen Moment dauern.

Wechselnde Validierungsergebnisse

- Symptom:
  - Das Gesamtergebnis von mehreren Validierungen von ein und derselben Datei ist mal "gelb" und mal "grün".
- Mögliche Ursache:
  - Die Prüfung des Zertifikats der Signatur erfolgt online zum Zeitpunkt der Validierung durch Anfrage bei einem oder mehreren Vertrauensdiensteanbietern. Es kann vorkommen, dass ein Server eines Vertrauensdiensteanbieters temporär nicht erreichbar ist. Dann kann die Validierung nicht vollständig durchgeführt werden und wird mit "gelb" bewertet. Das Prüfprotokoll weist auf die nicht erfolgreiche Online-Prüfung hin. Bitte wiederholen Sie in diesem Fall die Validierung zu einem späteren Zeitpunkt noch einmal.

Signaturprüfung der Serverantwort ist fehlgeschlagen

- Symptom:
  - Eine vermeintlich gültige Signatur wird nach der Validierung mit dem Gesamtergebnis "gelb" bewertet, weil die Vertrauenswürdigkeit des Vertrauensdiensteanbieters nicht ermittelt werden konnte. Im Prüfprotokoll ist der zusätzliche Abschnitt "Übertragungsinformation" vorhanden und enthält ein "rotes" Prüfergebnis.
- Mögliche Ursache:
  - Das Zertifikat zur Prüfung der Antwort des Validierungsdienst ist nicht korrekt, vgl. Kapitel 5.7. Bitte kontaktieren Sie den Betreiber des verwendeten Validierungsdienstes, um das korrekte Zertifikat zu erhalten.

Signaturalgorithmus ist nicht mehr geeignet

- Symptom:
  - Hinter der Bezeichnung des Signaturalgorithmus ist vermerkt, dass dieser nicht mehr für qualifizierte, elektronische Signaturen geeignet ist.
- Ursache:
  - Governikus DATA Boreum führt eine Bewertung der für die Signatur verwendeten Hash-Algorithmen durch. Die Bewertung basiert auf einem Algorithmenkatalog, der von der SOG-IS veröffentlicht wird. Governikus DATA Boreum enthält jeweils den Algorithmenkatalog, der zum Zeitpunkt der Erstellung der jeweiligen Version von Governikus DATA Boreum aktuell war.

Warnhinweis "Onlineprüfung ist abgewählt"

- Symptom:
  - Im Dialog "Validieren" wird unter "Validierungsdienst" der rote Warnhinweis "Validierung ohne Validierungsdienst" angezeigt.
- Ursache:
  - Die Prüfung einer qualifizierten elektronischen Signatur erfordert unter anderem, dass zum Zeitpunkt der Signaturprüfung "online" bei dem ausstellenden

Vertrauensdiensteanbieter erfragt werden muss, ob das zur Signatur verwendete Zertifikat zum Signaturzeitpunkt gültig oder gesperrt war. Diese Abfrage erfolgt über den Validierungsdienst. Ist die Online-Prüfung nicht konfiguriert, wird nur eine mathematische Signaturprüfung durchgeführt. Bitte tragen Sie in diesem Fall über den Dialog "Einstellungen" einen Validierungsdienst ein.

Ergebnisdatei kann nicht gedruckt werden

- Symptom:
  - Als Folgeanwendung wurde "Drucken" ausgewählt, aber es passiert nichts, bzw. die Datei wird nur geöffnet.
- Mögliche Ursache:
  - Für das Drucken werden die Einstellungen Ihres Betriebssystems verwendet. Das Drucken ist nur möglich, wenn für den Dateityp eine Verknüpfung mit dem Druckprogramm existiert. Ob eine Verknüpfung von Dateityp mit Druckprogramm vorhanden ist, können Sie überprüfen, in dem Sie im Datei-Explorer Ihres Rechners die Datei auswählen und das Kontextmenü öffnen. Ist dort die Option "Drucken" aufgeführt, existiert eine Verknüpfung.

Fehlermeldung "Die Datei wurde verändert"

- Symptom:
  - Beim Versuch eine Datei einzusehen, wird lediglich der Warnhinweis angezeigt, dass die Datei verändert wurde.
- Ursache:
  - Vorgang Signieren: Governikus DATA Boreum 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.
  - Vorgang Validieren: Governikus DATA Boreum stellt sicher, dass ein Prüfprotokoll zwischen Erstellung und Anzeige durch Governikus DATA Boreum nicht unbemerkt manipuliert werden kann. Wird der Warnhinweis angezeigt, kann die Integrität des vorliegenden Prüfprotokolls nicht gewährleistet werden. Bitte führen Sie in diesem Fall eine erneute Validierung durch.

12 Ablage von Daten bei Nutzung des Installers

12.1.1 Installation der Anwendung

Die Anwendung wird standardmäßig im lokalen Programm-Verzeichnis abgelegt.

Beispiel: `C:\Program Files (x86)\ Governikus KG\DATA Boreum`

Hinweise:

Die Anwender benötigen Vollzugriff auf dieses bzw. das gewählte Verzeichnis (Administrationsrechte).

12.1.2 Ablage von log-Informationen

Nach der Installation und dem Start der Anwendung werden im lokalen Temp-Ordner des Nutzer-Verzeichnisses Log-Informationen zum Installer und zur Anwendung abgelegt.

Ablageort Beispiel: "C:\Users\name\AppData\Local\Temp\Governikus KC\DATA Boreum“.

Wenn der Ort des Temp-Verzeichnisses nicht bekannt ist, kann dieser über den Windows Explorer mit der Eingabe „%Temp%“ gefunden werden. Im Temp-Ordner finden sich die Log-Dateien dann im Unterordner „Governikus KG“.

Log-Dateien:

xxx.err.log = Enthält alle Informationen zu Vorgängen, die der Installer ausführt (Versionsnummer des Installers, Informationen zu Systemeinstellungen, Prüfen auf neue Versionen etc.).

xxx.out.log = Enthält alle Informationen zur Anwendung (Version der Anwendung, enthaltene Anwendungsdateien, ausgeführte Funktionen etc.). Die enthaltenen Informationen sind vergleichbar mit denen der JWS-Konsole.

Hinweise: Treten bei der Nutzung der Anwendung Fehler auf, können die genannten Log-Dateien für die Fehlersuche herangezogen werden.

13 Barrierefreiheit

Dieses Kapitel beschreibt die in der Anwendung Governikus DATA Boreum umgesetzten Funktionalitäten, die sich aus den Anforderungen hinsichtlich der Barrierefreiheit ergeben.

Hinweis

Bevor ein Screen-Reader benutzt werden kann, muss zuerst die Java Access Bridge aktiviert werden

13.1 Java Access Bridge aktivieren

DATA Boreum wird mit einem eigenen 64 Bit Java ausgeliefert. Damit werden mögliche Konflikte mit anderen Java-basierten Programmen ausgeschlossen. Allerdings erfordert dies, dass die Java Access Bridge zweimal aktiviert werden muss, einmal im Windows Betriebssystem und einmal in DATA Boreum.

1. Java Access Bridge im Windows Betriebssystem aktivieren

Gehen Sie wie folgt vor:

- Klicken Sie auf den Windows-Start-Button und geben Sie „Systemsteuerung + Enter“ ein.
- Wählen Sie auf der Dialogseite „Systemsteuerung“ den Eintrag „Erleichterte Bedienung“.
- Wählen Sie im Abschnitt „Center für erleichterte Bedienung“ den Eintrag: „Visuelle Darstellung des Bildschirms aktivieren“.
- Blättern Sie auf der Seite “Erkennen von Bildschirmobjekten erleichtern“ nach ganz unten, und wählen Sie die Option „Java Access Bridge aktivieren“ aus.

2. Java Access Bridge für DATA Boreum aktivieren

Um die Java Access Bridge für das von DATA Boreum mitgelieferte Java zu aktivieren, gibt es zwei Möglichkeiten, die im Folgenden beschrieben werden:

Variante 1: Aktivieren mit Batch-Datei

Wechseln Sie im Windows Explorer in dieses Verzeichnis:

```
C:\Program Files (x86)\Governikus KG\DATA Boreum\jre64\bin
```

In diesem Verzeichnis finden Sie die Datei `accessibility_enable.bat`. Mit einem Doppelklick auf die Datei wird die Java Access Bridge für DATA Boreum aktiviert. Die Aktivierung erfolgt im Hintergrund und wird nicht angezeigt.

Variante 2: Aktivieren mit Kommandozeile

Gehen Sie in diesem Fall wie folgt vor:

- Öffnen Sie die Eingabeaufforderung (CMD).
- Wechseln Sie mit diesem Befehl in das Java-Verzeichnis von DATA Boreum. Die Anführungszeichen vor und hinter der Pfadangabe sind wichtig, da die Pfadangabe Leerzeichen enthält.:
- `cd "C:\Program Files (x86)\Governikus KG\DATA Boreum\jre64\bin"`
- Aktivieren Sie die Java Access Bridge mit diesem Befehl:

- `jabswitch -enable`

Das System antwortet mit der Zeile: `The Java Access Bridge has been enabled`. Danach können Sie das Fenster der Eingabeaufforderung/CMD wieder schließen. Dieser Vorgang muss nur einmal durchgeführt werden.

Hinweise:

Der Screen-Reader muss nach der Aktivierung der Java Access Bridge neu gestartet werden.

DATA Boreum muss nach Aktivierung der Java Access Bridge neu gestartet werden.

Achtung: Wenn DATA Boreum aktualisiert wurde, muss die Java Access Bridge für das Java von DATA Boreum erneut aktiviert werden.

13.2 DATA Boreum und die Umsetzung der Barrierefreiheit

Dieses Kapitel beschreibt die in der Anwendung Governikus DATA Boreum umgesetzten Funktionalitäten, die sich aus den Anforderungen hinsichtlich der Barrierefreiheit ergeben. Da es weder eine Norm noch einen gesetzlichen vorgeschriebenen Test der Barrierefreiheit von Softwareprodukten gibt, benutzt die Governikus KG die BITV-Tests. Die Benutzeroberfläche von Governikus DATA Boreum enthält weder Videosequenzen, noch CAPTCHAs oder Tonspuren. Deshalb sind einige der Prüfschritte des BITV-Tests nicht anwendbar. Die anwendbaren Prüfschritte werden, soweit möglich, durchgeführt. Die BITV-Tests sind für Web-Seiten erstellt worden, bei denen unter anderem auch bestimmte Aspekte des HTML-Codes geprüft werden. Diese Tests sind nur eingeschränkt anwendbar. Die Benutzeroberfläche von DATA Boreum wurde in Java Swing erstellt, daher es ist kein Zugriff auf den Programmcode möglich. Prüfwerkzeuge wie Colour Contrast Analyser oder NVDA werden zum Testen verwendet. Möglicherweise fehlende Aspekte der Barrierefreiheit werden regelmäßig geprüft und die Software laufend angepasst.

Umsetzung der Anforderungen

- **Screen-Reader**: Die Bedienung ist über einen Screen-Reader gewährleistet. Alle Elemente und Tooltips werden vorgelesen. Die Governikus KG hat dies mit NVDA und JAWS getestet. Wie ausführlich die Benutzeroberfläche vorgelesen wird, ist in den jeweiligen Screen-Reader-Programmen sehr genau einstellbar.
- **Navigation**: Die Navigation in der Benutzeroberfläche ist ohne Maus möglich. Es werden verschiedene Tasten und Tastenkombinationen angeboten, die in Tooltips angezeigt werden und im Anwendungshandbuch erklärt sind. Für jede Bediengruppe, wie beispielsweise die Menüleiste, wird vorgelesen, mit welchen Tasten oder Tastenkombinationen in dieser Gruppe navigiert werden kann.
- **Fokussierbarkeit**: Der Tastaturfokus ist sichtbar und wird durch eine Umrandung des aktiven Elements gekennzeichnet oder durch Invertierung der Farben.
- **Alternative-Texte**: Alle Bildelemente haben einen alternativen Text, der vorgelesen wird.

- **Skalierbarkeit der Schrift**: GUI-Texte können in drei verschiedenen Größen angezeigt werden.
- **Vergrößerung**: Die Vergrößerung der Benutzeroberfläche ist nicht mit dem Programm selbst steuerbar. Hierfür müssen die Bordmittel des Betriebssystems genutzt werden. Der Bildschirm ist beispielsweise bei Windows mit den Tasten Windows-Logo-Taste +Plus - Vergrößerung einschalten und Windows-Logo-Taste +ESC – Vergrößerung ausschalten, zu bedienen.
- **Kontraste**: Verbesserte Kontrastverhältnis sind umgesetzt: Die visuelle Darstellung von Text und Textbildern hat ein Kontrastverhältnis von mindestens 7:1. Folgende Ausnahmen gelten: großformatiger Text, dekorative Elemente, Logos. Für die Prüfung der Kontraste von benachbarten Farben wurde das Tool "Colour Contrast Analyser" eingesetzt.
- **Tabellen**: Bei Tabellen sind alle Rahmenlinien sichtbar. Tabellen sind nicht geschachtelt (nested), da bei geschachtelten Tabellen die Möglichkeit besteht, dass mit der Tastaturnavigation eine Endlosschleife (Tastaturfalle) entsteht.
- **Minimale Größe der Bedienelemente**: Klickbare GUI-Elemente sind immer groß genug und gewährleisten so eine Bedienung ohne punktgenaues Zielen.
- **Zustandsänderungen**: Werden Zustandsänderungen, Bedienhinweise und andere Meldungen durch Farben signalisiert (z. B. Ampelfarben), sind zusätzlich Symbole eingesetzt, da eine Farbänderung möglicherweise nicht wahrgenommen wird.

Im folgenden Kapitel ist dokumentiert, wie die Prüfschritte der BITV auf die GUI von Governikus DATA Boreum angewendet wurden. Jeder Prüfschritt ist kommentiert.

13.3 BITV-Test - Liste der Prüfschritte im Testverfahren

In der folgenden Tabelle werden alle Prüfschritte des BITV-Testverfahrens bezüglich ihrer Umsetzung in Governikus DATA Boreum bewertet. Die Software hat keine Videosequenzen, CAPTCHAs oder Tonspuren. Damit entfallen auch die Prüfschritte, die auf diese Multimedia-Inhalte abzielen und werden als Nichtzutreffend gekennzeichnet. Tests wurden unter anderem mit NVDA durchgeführt. NVDA steht für Non-Visual Desktop Access und ist ein Screen-Reader, der frei zu beziehen ist. Im Folgenden wird für die Benutzeroberfläche die Abkürzung GUI (Graphical User Interface) benutzt.

Technologie

Die Anwendung Governikus DATA Boreum ist in Swing umgesetzt, daher muss die Java Access Bridge aktiviert werden. Dies ist im Kapitel 13.1 erklärt. Danach können Screen-Reader wie NVDA sofort und ohne weitere Einstellungen bezüglich Java benutzt werden.

Java Swing ist nicht HTML. Viele BITV-Tests zielen auf die barrierefreie Umsetzung von HTML-Elementen ab, die nur zum Teil eine Entsprechung in Java Swing haben. Bei der Bewertung der Prüfschritte des BITV-Tests haben wir versucht, wenn vorhanden, die Java Swing-Entsprechungen von HTML so zu beschreiben, dass die Absicht des Prüfschritts auch auf die Benutzeroberfläche anwendbar ist. Dies wird mit dem Wort "Entsprechung" am Anfang der Zeile ausgedrückt.

Tabelle der Prüfschritte

Prüfschritt	Umsetzung in Governikus DATA Boreum
1.1.1 Nicht-Text-Inhalte	
1.1.1a Alternativtexte für Bedienelemente	Entsprechung: Alle grafischen Bedienelemente haben Alternativtexte, die die Funktion des Bedienelements beschreiben. Getestet mit NVDA.
1.1.1b Alternativtexte für Grafiken und Objekte	Entsprechung: Alle Grafiken haben alternative Texte, unabhängig davon, ob sie Bedienelemente sind, Zustände visualisieren oder Zusatzinformationen liefern. Hintergrundbilder, Icon Fonts und SVGs, sowie Video- beziehungsweise Audio-Dateien oder Applets sind nicht in die GUI eingebunden.

Prüfschritt	Umsetzung in Governikus DATA Boreum
1.1.1c Leere alt-Attribute für Layout-Grafiken	Nichtzutreffend: Da die Anwendung Java und nicht HTML ist, gibt es keine Layout-Grafiken, die zur Gestaltung der Benutzeroberfläche eingefügt wurden und vorgelesen werden könnten.
1.1.1d Alternativen für CAPTCHAs	Nichtzutreffend: Die Anwendung enthält keine CAPTCHAs.
1.2.1 Aufgezeichnete Audio- und Video-Dateien	
1.2.1a Alternativen für Audiodateien und stumme Videos	Nichtzutreffend: Die Anwendung enthält keine Videos, daher sind auch keine gleichwertige Medienalternativen vorhanden.
1.2.2 Erweiterte Untertitel (Captions)	
1.2.2a Aufgezeichnete Videos mit Untertiteln	Nichtzutreffend: Die Anwendung enthält keine Videos, daher werden auch keine Captions/Untertitel verwendet.
1.2.3 Audio-Deskription oder Volltext-Alternative	
1.2.3a Audiodeskription oder Volltext-Alternative für Videos	Nichtzutreffend: Die Anwendung enthält keine Videos, daher sind keine Audiodeskriptionen oder Volltext-Alternativen enthalten.
1.2.4 Live-Untertitel	
1.2.4a Videos (live) mit Untertiteln	Nichtzutreffend: Die Anwendung enthält keine Live-Videos und daher auch keine synchronen Untertitel.
1.2.5 Audio-Deskription	
1.2.5a Audiodeskription für Videos	Nichtzutreffend: Die Anwendung enthält keine Videos und daher werden auch keine Audiodeskriptionen benötigt.

Hinweis: Der Abschnitt 1.3.1 behandelt die Prüfung der korrekten Umsetzung von HTML-Tags. Es gibt für die HTML-Tags Entsprechungen in Java Swing. Deren korrekte Umsetzung wird durch den Java-Compiler geprüft. Eine Überprüfung mit den empfohlenen Bookmarklets ist für Java-Programme nicht möglich.

1.3.1 Informationen und Beziehungen	
1.3.1a HTML-Strukturelemente für Überschriften	Entsprechung: Die GUI enthält keine Überschriften. Jeder Dialogseite hat einen Namen, der beim Öffnen der Dialogseite vorgelesen wird.
1.3.1b HTML-Strukturelemente für Listen	Entsprechung: In Java Swing werden Listen mit der Klasse `ListView` dargestellt. Eine Kontrolle mit Bookmarklets ist nicht möglich. Eine so erzeugte Liste wird Zeilenweise vorgelesen. Die Pfeil-Taste führt zur nächsten Zeile. Es gibt keine verschachtelten Listen. Die Navigation in Listen ist mit Pfeilen umgesetzt. Tab-Taste führt zu dem nächsten GUI-Element.
1.3.1c HTML-Strukturelemente für Zitate	Nichtzutreffend: Die GUIs von Software der Governikus KG enthalten keine Zitate.
1.3.1d Inhalte gegliedert	Nichtzutreffend: Dieser Prüfschritt bezieht sich auf Fließtext, der in hintereinander folgenden Absätzen unterteilt ist. Es gibt in der GUI keine längeren Fließtexte.
1.3.1e Datentabellen richtig aufgebaut	Entsprechung: Die korrekte Formatierung einer Tabelle wird vom Java Swing-Compiler geprüft. Es gibt keine geschachtelten Tabellen. Tabellen werden zeilenweise mit den Pfeil-Tasten "durchschritten". Tab-Taste führt zu dem nächsten GUI-Element.
1.3.1f Zuordnung von Tabellenzellen	Nicht anwendbar: Der Prüfschritt ist nicht anwendbar, da in der GUI keine komplexen Tabellen enthalten sind. Ein verständliche Erklärung zu komplexen Tabellen findet sich auf der Webseite Web Usability von Roger Hudson.

1.3.1 Informationen und Beziehungen	
1.3.1g Kein Strukturmarkup für Layout-Tabellen	Nichtzutreffend: In der GUI werden keine Tabellen für das Layout benutzt.
1.3.1h Beschriftung von Formularelementen programmatisch ermittelbar	Entsprechung: Die GUI ist in Java Swing so programmiert, dass für alle GUI-Elemente, die eine Beschriftung haben, immer eine eindeutige Zuordnung zwischen der Beschriftung und dem beschrifteten GUI-Element besteht. Dies wurde mit dem Screen-Reader geprüft.

1.3.2 Aussagekräftige Reihenfolge	
1.3.2a Sinnvolle Reihenfolge	Entsprechung: Die Abfolge der GUI-Elemente ist in einer sinnvollen Reihenfolge mit den Mitteln von Java Swing programmiert. Dies wurde mit Tab-Navigation vorwärts sowie rückwärts geprüft. Da ein abschalten von "Styles/CSS" in einer Java-GUI nicht möglich ist, ist dieser Teil des Prüfschritts nichtzutreffend.
1.3.3 Sensorische Merkmale	
1.3.3a Ohne Bezug auf sensorische Merkmale nutzbar	Entsprechung: Da die Funktionen aller GUI-Elemente und deren Eingabemöglichkeiten vorgelesen werden, gibt es keine Elemente, die nur über ihre Farbe, Form, Größe, Position, oder Orientierung erfassbar sind.
1.3.4 Ausrichtung	
1.3.4a Keine Beschränkung der Bildschirmausrichtung	Entsprechung: Ob der Bildschirm horizontal oder vertikal ausgerichtet ist, ist für die GUI unerheblich, da diese nie den gesamten Bildschirm einnimmt. Die Fenstergröße der GUI ist in einem sinnvollen Umfang skalierbar.
1.3.5 Zweck von Eingaben bestimmen	

1.3.2 Aussagekräftige Reihenfolge	
1.3.5a Eingabefelder zu Nutzerdaten vermitteln den Zweck	Entsprechung: Für jedes Eingabefeld gibt es einen Tooltip, mit dem erklärt wird, was, und gegebenenfalls in welchem Wertebereich, eingegeben werden soll. Wo dies möglich ist erleichtern Drop-down-Listen die Eingabe.
1.4.1 Farbe	
1.4.1a Ohne Farben nutzbar	Entsprechung: Farben dienen nur dem Design. Die gesamte GUI ist vollständig ohne Farbinformation nutzbar, wie z.B. mit Style/Kontrast. Fettdruck wird nur für das Design verwendet und hat keine Semantik.
1.4.2 Audio-Kontrolle	
1.4.2a Ton abschaltbar	Nichtzutreffend: Die GUI enthält keine eingebetteten Audio-Medien. Benutzer sind daher nicht auf Ton angewiesen.
1.4.3 Kontrast	
1.4.3a Kontraste von Texten ausreichend	Entsprechung: Das Kontrastverhältnis zwischen GUI-Text und Hintergrund wurde mit dem Tool Colour Contrast Analyser geprüft und auf einen verbesserten Kontrast 7:1 eingestellt.
1.4.4 Veränderbare Textgröße	
1.4.4a Text auf 200% vergrößerbar	Entsprechung: Die Textgröße der GUI-Texte lässt sich über das entsprechende Menü zwischen der kleinsten und der größten Einstellung um 130% vergrößern. Für eine stärkere Vergrößerung müssen die Bordmittel des Betriebssystems genutzt werden. Bei Windows lässt sich beispielsweise mit den Tasten Windows-Logo-Taste +Plus – die Vergrößerung einschalten und Windows-Logo-Taste +ESC – Vergrößerung ausschalten. Die Vergrößerungsstufe ist dabei per Default 200%. Diese Stufe ist einstellbar.
1.4.5 Schriftgrafiken	

1.3.2 Aussagekräftige Reihenfolge	
1.4.5a Verzicht auf Schriftgrafiken	Nichtzutreffend: In der GUI gibt es keine Schriften auf Grafiken.
1.4.10 Umbruch	
1.4.10a Inhalte brechen um	Entsprechung: Längere Texte, die die hier gewünschte Eigenschaft "responsives Verhalten bei Größenveränderungen der GUI" aufweisen sollen, gibt es in der GUI nicht.
1.4.11 Nicht-Text Kontrast	
1.4.11a Kontraste von Grafiken und Bedienelementen ausreichend	Entsprechung: Grafiken werden in der GUI nur für Schaltflächen eingesetzt. Alle Grafiken sind durch eine schwarze Umrandung vom Hintergrund abgehoben. Alle Grafiken haben alternativen Text, der vorgelesen werden kann. Alle Grafiken haben Tooltips, die die Beschriftung der Schaltfläche angeben, wenn der Mauszeiger auf die Grafik zeigt. Damit ist die vollständige, kontrastharte Darstellung auf den Schaltflächen für die Erfassung von deren Bedeutung nicht wichtig, da es mehrere alternative Wege gibt, die Schaltflächen in der GUI zu erfassen.
1.4.12 Textabstände	
1.4.12a Textabstände anpassbar	Entsprechung: Die GUI enthält keinen Fließtext, der in dieser Form angepasst werden müsste.
1.4.13 Eingeblendete Inhalte	
1.4.13a Eingeblendete Inhalte bedienbar	Entsprechung: Die einzigen Informationen, die durch Zeigen auf GUI-Elemente mit der Maus angezeigt werden, sind Tooltips von Schaltflächen. Diese werden, weil sie nur sehr kurze Texte enthalten, nach 5 Sekunden wieder ausgeblendet, um eine zügige Bedienung der GUI zu ermöglichen. Die Texte können, durch erneutes Zeigen auf das Element, immer wieder erneut zur Anzeige gebracht werden.

1.3.2 Aussagekräftige Reihenfolge	
	Allein durch Zeigen mit der Maus werden keine Bedienelemente angezeigt. Dies erfordert immer ein explizites Klicken auf das GUI-Element. Drop-down-Listen werden beispielsweise solange angezeigt, bis eine Auswahl getroffen wurde. Ein automatisches Einklappen nach einem voreingestellten Timeout gibt es nicht. Wird die Drop-down-Liste durch Klicken mit oder ohne Auswahl geschlossen, bleibt der Fokus erhalten.
2.1.1 Tastaturbedienbarkeit	
2.1.1a Ohne Maus nutzbar	Entsprechung: Die GUI ist nahezu vollständig und ohne Einschränkung über die Tastatur bedienbar. Der Screen-Reader liest zusätzlich die Möglichkeiten der Bedienung vor, die in der Oberfläche der GUI hinterlegt sind.
2.1.2 Keine Tastaturfalle	
2.1.2a Keine Tastaturfalle	Entsprechung: Tastaturfallen entstehen beispielsweise durch verschachtelte Tabellen, die es in der GUI nicht gibt. Alle Formularelemente können erreicht und auch wieder verlassen werden. Links zu anderen Websites sind nicht in der GUI enthalten. Die einzigen Links finden sich im Prüfprotokoll. Diese Links verweisen auf Ziele innerhalb derselben Seite und können daher keine Tastaturfalle sein.
2.1.4 Tastaturkurzbefehle	
2.1.4a Tastatur-Kurzbefehle abschaltbar oder anpassbar	Entsprechung: In der GUI werden nur Tastaturkurzbefehle benutzt, die allein oder mit den üblichen Steuertasten Strg, Alt, Enter, Tab, Pfeiltasten und Funktionstasten kombiniert werden. Es wurde getestet, dass keine andere Taste eine ungewollte Aktion auslösen kann. Wir gehen davon aus, dass es bei einer Sprachsteuerung des Programms keine Probleme mit Tastaturkurzbefehlen gibt.
2.2.1 Zeitbezogene Anforderungen	
2.2.1a Zeitbegrenzungen anpassbar	Nichtzutreffend: Es gibt keine Timeouts in der GUI. Der einzige Vorgang, der ein Timeout hat, ist das Anbringen einer qualifizierten elektronischen Signatur mit

1.3.2 Aussagekräftige Reihenfolge	
	einem dafür geeigneten Chipkartenleser. Hier wird zur Eingabe aufgefordert. Der hier eingestellte Abbruch des Vorgangs bei Zeitüberschreitung, kann von der Governikus KG nicht beeinflusst werden und hat Sicherheitsgründe.
2.2.2 Anhalten, beenden, ausblenden	
2.2.2a Bewegte Inhalte abschaltbar	Nichtzutreffend: Die GUI enthält keine blinkenden oder bewegte GUI-Elemente.
2.3.1 Dreimaliges Aufblitzen – Unterschreiten der Schwellenwerte	
2.3.1a Verzicht auf Flackern	Nichtzutreffend: Die GUI enthält keine blinkenden oder aufflackernden Elemente.
2.4.1 Umgehen von Elementgruppen	
2.4.1a Bereiche überspringbar	Entsprechung: Semantisch zusammenhänge Gruppen werden über die Tab-Taste erreicht. Die Tab-Taste ermöglicht somit das Überspringen von gruppierten GUI-Elementen. Auch gruppierte GUI-Elemente werden vorgelesen. Da es keine Fleißtexte mit Überschriften gibt, trifft dieser Teil des Prüfschritts nicht zu.
2.4.2 Webseiten-Titel	
2.4.2a Sinnvolle Dokumenttitel	Entsprechung: Jede Dialogseite der GUI hat einen eigenen, individuellen Titel, der vorgelesen wird.
2.4.3 Fokus-Reihenfolge	
2.4.3a Schlüssige Reihenfolge bei der Tastaturbedienung	Entsprechung: Die Reihenfolge wird durch die Bedienlogik vorgegeben. Je nach Auswahl in der Menüleiste oder dem Durchschreiten der Dialogseite, werden die GUI-Elemente in der Reihenfolge angesteuert, die sich aus der sinnvollen Benutzung des Programms ergibt.

1.3.2 Aussagekräftige Reihenfolge	
2.4.4 Zweck eines Links (im Kontext)	
2.4.4a Aussagekräftige Linktexte	Die Benutzeroberfläche ist keine HTML-Seite von der aus über Links auf andere Quellen oder Seiten verwiesen wird. Mit dem Fehlen dieser Links entfällt auch die Angabe aussagekräftiger Hinweise zu den Sprungzielen und mögliche Hinweise darauf, ob der Link in einer neuen Instanz (neue Browserseite, neue Client-GUI) geöffnet wird.
2.4.5 Alternative Zugangswege	
2.4.5a Alternative Zugangswege	Nichtzutreffend: Da der Client mit seiner GUI kein Angebot einer Website ist, wird der Inhalt und die Benutzungsreihenfolge über Maus- oder Tastatursteuerung erschlossen. Alle für die Bearbeitung eines Benutzungsschritts notwendigen GUI-Elemente befinden sich auf einer Dialogseite.
2.4.6 Beschreibungen	
2.4.6a Aussagekräftige Überschriften und Beschriftungen	Entsprechung: Alle GUI-Elemente einer Dialogseite haben eine kurze und beschreibende Beschriftung. Schalflächen und Eingabefelder enthalten Tooltips mit weiterführenden Kontextinformationen. Für komplexe Vorgänge, die sich nicht über die GUI erschließen, sollte die barrierefreie PDF-Dokumentation hinzugezogen werden. Komplexe Fragestellungen, wie beispielsweise, was ist eine qualifizierte elektronische Signatur, welche rechtlichen Konsequenzen sind damit verbunden und wo wird sie eingesetzt, können nicht über GUI-Elemente erklärt werden und sind daher in der Produktdokumentation erklärt.
2.4.7 Sichtbarer Fokus	
2.4.7a Aktuelle Position des Fokus deutlich	Entsprechung: Der aktuelle Fokus in der GUI wird bei Nutzung mit Screen-Reader immer vorgelesen und ist durch einen eine schwarze Umrandung des GUI-Elements optisch hervorgehoben. Links existieren nur im Prüfprotokoll für

1.3.2 Aussagekräftige Reihenfolge	
	Sprungziele innerhalb desselben Dokuments. Diese Links sind unterstrichen und werden beim Erreichen vorgelesen.
2.5.1 Zeigergesten	
2.5.1a Alternativen für komplexe Zeiger-Gesten	Nichtzutreffend: Für die GUI ist keine Gestensteuerung implementiert. Die Bedienung erfolgt ausschließlich über die Maus und die Tastatur.
2.5.2 Abbruch von Zeigergesten	
2.5.2a Zeigergesten-Eingaben können abgebrochen oder widerrufen werden	Nichtzutreffend: Für die GUI ist keine Gestensteuerung implementiert, daher kann sie auch nicht abgebrochen werden. Die Bedienung erfolgt ausschließlich über die Maus und die Tastatur.
2.5.3 Beschriftung im zugänglichen Namen	
2.5.3a Sichtbare Beschriftung Teil des zugänglichen Namens	Entsprechung: Alle sichtbaren GUI-Texte für Beschriftungen von Bedienelementen, werden genauso vorgelesen, wie sie sichtbar beschriftet sind. Der sichtbare Name ist auch der Name des Bedienelements.
2.5.4 Bewegungsaktivierung	
2.5.4a Alternativen für Bewegungsaktivierung	Nichtzutreffend: Eine Steuerung des Clients durch Bewegung des Geräts ist nicht implementiert. Ebenfalls gibt es keine Eingabemöglichkeit durch angeschlossene Geräte, die über Bewegungen gesteuert werden, außer der Computermaus und der Tastatur.
3.1.1 Sprache	
3.1.1a Hauptsprache angegeben	Entsprechung: Bei Java Swing wird die Sprache in einer Datei namens application.xml festgelegt. Da diese Datei vom Screen-Reader nicht gelesen wird,

1.3.2 Aussagekräftige Reihenfolge	
	muss zum Festlegen der Hauptsprache die Ausgabesprache in den Einstellungen des Screen-Readers festgelegt werden.
3.1.2 Sprache einzelner Abschnitte	
3.1.2a Anderssprachige Wörter und Abschnitte ausgezeichnet	Nichtzutreffend: Dies ist mit Mitteln von Java Swing nicht umsetzbar. Es ist möglich, im Screen-Reader Transkriptionen für Wörter anzugeben, damit diese vom Screen-Reader korrekt vorgelesen werden, Beispiel sind: HTML → H T M L Release → Relies Signaturniveau → Signaturnivoh Aktuell wird der Import eines angepassten Standardwörterbuchs von NVDA nicht direkt unterstützt. Es ist möglich eine portable Version von NVDA zu erstellen. In dieser Variante kann eine Datei `default.dic` hinterlegt werden. Diese Datei kann dann Transkriptionen für Wörter enthalten, die eine andere Aussprache erfordern. Dieses Vorgehen müsste mit den interessierten Anwendern abgesprochen werden, da diese möglicherweise Anpassungen vorgenommen haben, die durch einen Austausch der Datei `default.dic` verloren gehen. Es ist auch möglich eine Liste der Transkriptionen auszuliefern, die dann von den Anwendern zeilenweise in das Standardwörterbuch übertragen wird. Dieser Weg ist für Anwender sehr aufwendig.
3.2.1 Bei Fokussierung	
3.2.1a Keine unerwartete Kontextänderung bei Fokus	Entsprechung: Wenn für das Arbeiten mit DATA Boreum ein neues Fenster geöffnet werden muss, wird dies über den Button-Text, der das Fenster aufruft, vorgelesen.
3.2.2 Bei Eingabe	

1.3.2 Aussagekräftige Reihenfolge	
3.2.2a Keine unerwartete Kontextänderung bei Eingabe	Entsprechung: Kontextänderungen werden durch die Auswahl von Optionen von Menüs und anderen Bedienelementen erwartungskonform durchgeführt. Eine automatische Änderung des Kontexts bei Eingabe oder ohne Bedienelemente findet nicht statt.
3.2.3 Einheitliche Navigation	
3.2.3a Konsistente Navigation	Entsprechung: Die GUI ist kein Webauftritt; sie garantiert eine durchgängige Bedienung und hat eine hohe Lernkurve durch konsistente und wiederkehrende Navigations- und Bedienelemente.
3.2.4 Einheitliche Bezeichnung	
3.2.4a Konsistente Bezeichnung	Entsprechung: Bezeichnungen in der GUI sind konsistent. Wechselnde Funktionen ändern nicht die Bezeichnungen für die Navigation oder Bedienung. Gleich Funktionen in verschiedenen Dialogseiten sind gleich bezeichnet.
3.3.1 Fehleridentifizierung	
3.3.1a Fehlererkennung	Entsprechung: Fehlende oder falsche Eingaben werden mit einem roten Rahmen versehen. Der Screen-Reader liest bei fehlenden oder falschen Eingaben vor, welches Feld betroffen ist, welche Eingabe erwartet wurde und welcher Fehler vorliegt.
3.3.2 Beschriftungen	
3.3.2a Beschriftungen von Formularelementen vorhanden	Entsprechung: Alle Formularelemente sind entweder vor oder über dem Feld beschriftet und werden vom Screen-Reader vorgelesen. Ein Tooltip erklärt die erforderliche und erwartete Eingabe. Auch der Tooltip wird vorgelesen.
3.3.3 Korrekturvorschläge	

1.3.2 Aussagekräftige Reihenfolge	
3.3.3a Hilfe bei Fehlern	Entsprechung: Fehlende oder falsche Eingaben werden mit einem roten Rahmen versehen. Der Screen-Reader liest bei fehlenden oder falschen Eingaben vor, welches Feld betroffen ist, welche Eingabe erwartet wurde und welcher Fehler vorliegt.
3.3.4 Fehlervermeidung	
3.3.4a Fehlervermeidung wird unterstützt	Entsprechung: Ein Formular lässt sich nicht erfolgreich abschließen, solange Pflichteinträge fehlen oder falsch sind. Fehlende oder falsche Eingaben werden mit einem roten Rahmen versehen. Der Screen-Reader liest bei fehlenden oder falschen Eingaben vor, welches Feld betroffen ist, welche Eingabe erwartet wurde und welcher Fehler vorliegt.
4.1.1 Syntaxanalyse	
4.1.1a Korrekte Syntax	Entsprechung: Die Überprüfung der Korrektheit wird der Syntax wird vom Java Swing-Compiler geprüft.
4.1.2 Name, Rolle, Wert	
4.1.2a Name, Rolle, Wert verfügbar	Entsprechung: Die Bedienelemente der GUI ändern sich nicht. Sie bleiben statisch und haben keine interaktive Umsetzung, die kontextabhängig zu neuer Funktionalität führen könnten. Daher gilt die Beschriftung und Bediensemantik wie angegeben.
4.1.3 Statusmeldungen	
4.1.3a Statusmeldungen programmatisch verfügbar	Entsprechung: Die GUI gibt überwiegend optisches und akustisches Feedback. Fehlende oder falsche Eingaben werden rot umrandet und der Fehler wird vom Screen-Reader vorgelesen. Hier sind allerdings noch nicht alle Ereignisse abgedeckt. Diese werden bei zukünftigen Releases berücksichtigt und implementiert.

14 Abbildungsverzeichnis

Abbildung 1: Startdialog der Installation 11
Abbildung 2: Nutzungsbedingungen von Governikus DATA Boreum akzeptieren 12
Abbildung 3: Auswahl des Installationsverzeichnisses 12
Abbildung 4: Vorbereitung der Installation abgeschlossen 13
Abbildung 5: Installation fertigstellen 13
Abbildung 6: Update-Dialog mit Beispiel-Versionen 15
Abbildung 7: Verbindung zum Update-Server nicht möglich 15
Abbildung 8: Dialogseite zur Eingabe des Lizenzschlüssels 16
Abbildung 9: Aufforderung zum Neustart nach Lizenzschlüsseleingabe 17
Abbildung 10: Warnhinweis bei ungültigem Lizenzschlüssel 17
Abbildung 11: Registerkarte Allgemein im Einstellungsdialog 21
Abbildung 12: Programme verwalten 22
Abbildung 13: Programm hinzufügen oder bearbeiten 23
Abbildung 14: Registerkarte Anwendungen 24
Abbildung 15: Registerkarte Signieren 25
Abbildung 16: Registerkarte Governikus 27
Abbildung 17: Registerkarte BNotK 28
Abbildung 18: Dialogabschnitt "Soll ein Signaturfeld sichtbar sein?" 29
Abbildung 19: Vorlagennamen eingeben 30
Abbildung 20: Vorlagen verwalten mit Beispielvorlagen 30
Abbildung 21: Dialogabschnitt "Zusätzliche Unterschriftsinformationen" 31
Abbildung 22: Beispiele für eine Visualisierung mit Grafik und Text 32
Abbildung 23: Dialogabschnitt "Signaturfeld platzieren" 32
Abbildung 24: Registerkarte PDF im Dialog "Einstellungen" 34
Abbildung 25: Registerkarte Validierung 36
Abbildung 26: Registerkarte Netzwerk mit Beispieldaten 39
Abbildung 27: Einstiegsseite von Governikus DATA Boreum 43
Abbildung 28: Dialogseitenauswahl am Beispiel Signieren 45
Abbildung 29: DATA Boreum Kontextmenü im Windows Explorer 47
Abbildung 30: Hinweisdialog zum Prozesswechsel 47
Abbildung 31: Dialogseite Zielverzeichnis wählen 49
Abbildung 32: Kontextmenü in der Dateiauswahl 50
Abbildung 33: Dialogseite zum Anlegen von Signaturfeldern 53
Abbildung 34: Auswahl „Schlüssel aus Datei laden“ 57
Abbildung 35: Auswahl „Schlüssel von Signaturkarte“ 58

Abbildung 36: Auswahl Signaturdienst und Login-Dialog für den Authentisierungsdienst 60
Abbildung 37: Auswahl des BNotK Fernsignaturdienstes 61
Abbildung 38: Login-Dialog für den Authentisierungsdienst.....65
Abbildung 39: Letzte Dialogseite der Funktion Signieren.....67
Abbildung 40: Dialogfenster Prüfzeitpunkt auswählen 72
Abbildung 41: Letzte Dialogseite der Funktion Validieren.....74
Abbildung 42: Eingabe eines trivialen Passworts - wenige rote Punkte.....80
Abbildung 43: Eingabe eines ausreichend sicheren Passworts - alle Punkte grün.....80
Abbildung 44: Letzte Dialogseite der Funktion Verschlüsseln 81
Abbildung 45: Letzte Dialogseite der Funktion Entschlüsseln.....85
Abbildung 46: Zusätzlicher Eintrag im Startmenü 88
Abbildung 47: Kontextmenü von Governikus DATA Boreum im Tray 89
Abbildung 48: Optionen des Governikus DATA Boreum Tray-Icons.....92