Schnelleinstieg Dateien signieren

Was leistet eine elektronische Signatur?

Mit der Signatur einer Datei kann nachgewiesen werden, wer die Datei signiert hat (Authentizität) und ob die Datei nach dem Anbringen der Signatur verändert wurde (Integrität). Eine elektronische Signatur bezieht sich immer auf genau eine Datei. Die Signatur kann in der Datei selbst enthalten sein oder als zusätzliche Datei erstellt werden.

Welche Fälle werden betrachtet?

Prinzipiell kann jede Datei signiert werden. Dieser "Schnelleinstieg Dateien signieren" erklärt die folgenden Varianten:

- **PDF-Datei signieren**: Der mit weitem Abstand häufigste Anwendungsfall ist das Signieren einer PDF-Datei. Bei PDF-Dateien wird die Signatur innerhalb der Datei angebracht. Die Datei kann auch nach dem Signieren mit jedem PDF-Reader angeschaut werden.
- **Detached Signatur**: Der zweithäufigste - aber schon eher seltene - Fall ist das Signieren einer Datei, für die die Signatur in einer eigenen Datei erstellt wird. Ist das Ergebnis der Signaturerstellung die Originaldatei und eine Signaturdatei, wird die Signatur "detached" genannt, dabei bedeutet detached "freistehend".

Es gibt noch weitere Methoden der Signaturerstellung, die in diesem Schnelleinstieg nicht erklärt werden. Für diese Fälle lesen Sie bitte das "Governikus Signer Benutzerhandbuch".

Inhalt

Dieser Schnelleinstieg soll folgendes leisten:

- **Schnelleinstieg Dateien signieren**: Hier werden die Funktionen der Software Governikus Signer für das einfache Signieren von Dateien erklärt, siehe Kapitel 1.
- **Technisches Voraussetzungen**: Hier wird aufgeführt, welche Voraussetzungen erfüllt sein müssen, damit Sie Dateien signieren können, siehe Kapitel 2.
- **Grundverständnis**: Dieses Kapitel gibt eine kurze Einführung für ein technisches Grundverständnis des Signierens von Dateien, wobei kein Fachwissen vorausgesetzt wird, siehe Kapitel 3.

1 Signieren mit dem Governikus Signer

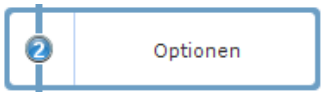
Stellen Sie sicher, dass die Hardware- und Software-Voraussetzungen erfüllt sind, siehe Kapitel 2. Rufen Sie den Governikus Signer auf und führen Sie die folgenden Schritte aus.

Funktion Signieren aufrufen

Klicken Sie auf der Startseite des Governikus Signer auf "Signieren". 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.

Ein oder mehrere Dateien auswählen

Wählen Sie über den Button "Datei hinzufügen" eine oder mehrere Dateien aus, die Sie signieren wollen. Sie können auch im Dateimanager eine oder mehrere Dateien auswählen und aus dem Kontextmenü "Governikus Signer - Signieren" wählen.



Signaturformat auswählen

Wählen Sie im Dialogabschnitt "Standardsignatur wählen (CAdES)" die Option "Signatur als gesonderte Datei beifügen (detached)". Mit dieser Auswahl bestimmen Sie das Signaturformat für alle Dateitypen außer PDF-Dateien. Diese werden im nächsten Dialogabschnitt behandelt.

Wählen Sie im Dialogabschnitt "Signieren von PDF-Dokumenten (PAdES)" die Option "PDF-Signatur erstellen" aus. Das Feld "Signaturfeld-Vorlage" ist eine Drop-down-Liste. Die Voreinstellung ist "Keine". Übernehmen Sie diese Auswahl. Lassen Sie das Feld "Grund der Unterschrift" leer.

Signaturniveau und Schlüssel wählen

Signaturniveau

Die Entscheidung, welches Signaturniveau Sie wählen, hängt davon ab, ob Sie ein Signaturzertifikat von einer Zertifikatsspeicherdatei oder von einer Signaturkarte benutzen wollen. Der Unterschied zwischen Signaturkarte und Zertifikatsspeicherdatei ist in Kapitel 3 erklärt. Im Dialogabschnitt "Signaturniveau" haben Sie diese Auswahl:

- **Alle**: Wenn Sie die Option "Alle" wählen, werden im darunter liegenden Dialogabschnitt alle angeschlossenen Chipkartenleser angezeigt, in denen eine Signaturkarte eingesteckt ist und es wird die Möglichkeit angezeigt, eine Zertifikatsspeicherdatei auszuwählen.
- **Qualifiziert**: Wenn Sie die Option "Qualifiziert" auswählen, werden im darunter liegenden Dialogabschnitt nur angeschlossene Chipkartenleser angezeigt, in denen eine Signaturkarte eingesteckt ist. Auf der Signaturkarte **muss** ein Signaturzertifikat für qualifizierte elektronische Signaturen enthalten sein. Die Möglichkeit, eine Zertifikatsspeicherdatei auszuwählen ist ausgegraut, denn nur Signaturen, die mit einer Signaturkarte erstellt wurden, sind qualifizierte elektronische Signaturen.
- **Fortgeschritten**: Wenn Sie die Option "Fortgeschritten" wählen, haben Sie im darunter liegenden Dialogabschnitt diese Auswahl:

- **Chipkartenleser**: Es werden alle angeschlossenen Chipkartenleser angezeigt, in denen eine Signaturkarte eingesteckt ist. **Hinweis**: Es werden nur die Chipkartenleser angezeigt, in denen eine Signaturkarte mit einem Zertifikat steckt, mit dem nur fortgeschrittene Signaturen erstellt werden können.
- **Zertifikatsspeicherdatei**: Zudem wird die Möglichkeit angezeigt eine Zertifikatsspeicherdatei auszuwählen.

	**Empfehlung**: Benutzen Sie zum Signieren eine Signaturkarte und wählen Sie das Signaturniveau "Qualifiziert". Das Ergebnis ist eine qualifizierte elektronische Signatur, die der handschriftlichen Unterschrift rechtlich gleichgestellt ist.

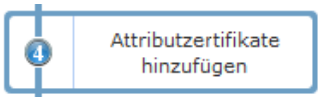
Speicherort des Schlüssels

Abhängig von der Auswahl des Signaturniveaus können Sie hier jetzt den Schlüssel wählen, mit dem die Dateien signiert werden sollen.

- **Chipkartenleser**: Es werden alle Chipkartenleser angezeigt, in denen eine Signaturkarte eingesteckt ist. Wählen Sie den Chipkartenleser mit der Signaturkarte aus, mit der die Dateien signiert werden sollen. Als nächstes wird geprüft ob das Signaturzertifikat auf der Signaturkarte noch gültig ist oder nicht. Mit einem Signaturzertifikat, dessen Gültigkeitszeitraum abgelaufen ist, kann nicht signiert werden. Nach dieser Auswahl werden im darunterliegenden Dialogabschnitt "Schlüsselauswahl" alle Zertifikate angezeigt, die auf der Signaturkarte gefunden wurden. Wählen Sie das Signaturzertifikat aus. Damit ist die Auswahl auf dieser Dialogseite abgeschlossen.

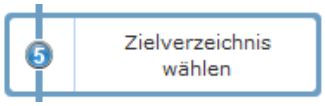
	**Hinweis**: Wenn Sie einen Personalausweis haben, der nach dem 01.11.2010 ausgestellt wurde und wenn Sie ein Signaturzertifikat auf den Personalausweis geladen haben, können Sie auch diesen zum Signieren auswählen. Lesen Sie dazu das "Governikus Signer Benutzerhandbuch".

- **Schlüssel aus Datei laden**: Wenn Sie diese Auswahl anklicken, wird ein Dateiauswahldialog angezeigt, mit dem Sie eine Zertifikatsspeicherdatei von Ihrem Dateisystem auswählen können. Eine Zertifikatsspeicherdatei hat die Endung `.p12` oder `.pfx`. Wenn Sie eine Zertifikatsspeicherdatei ausgewählt haben, wird direkt danach ein Dialogfenster angezeigt, in dem Sie die PIN eingegeben müssen, mit der die Zertifikatsspeicherdatei geschützt ist. Als nächstes wird geprüft ob das Signaturzertifikat in der Zertifikatsspeicherdatei noch gültig ist oder nicht. Mit einem Signaturzertifikat, dessen Gültigkeitszeitraum abgelaufen ist, kann nicht signiert werden. Damit ist die Auswahl auf dieser Dialogseite abgeschlossen.



Sonderfall Attributzertifikat

Der Sonderfall Attributzertifikat wird hier nicht weiter beschrieben. Für Informationen zu diesem Sonderfall lesen Sie bitte das "Governikus Signer Benutzerhandbuch".



Zielverzeichnis wählen

Wählen Sie hier das Verzeichnis aus, in dem die signierten Dateien gespeichert werden sollen. Sie haben die folgenden Möglichkeiten:

- **Quellverzeichnis nutzen**: Wenn Sie diese Optionen wählen, werden die signierten Dateien in dem Verzeichnis gespeichert, aus dem die Originaldatei stammt.
- **Zielverzeichnis wählen**: Wenn Sie diese Optionen wählen, wird ein Dateiauswahldialog geöffnet. Wählen Sie das Verzeichnis aus, in dem die signierten Dateien gespeichert werden sollen.

Dialogseite Signieren

Wenn alle Einstellungen vorgenommen wurden, können Sie jetzt mit dem Button "Signieren" das Signieren der angezeigten Dateien auslösen.

- **Signieren mit Signaturkarte**: Wenn Sie mit einer Signaturkarte signieren, müssen Sie für jede Datei, die signiert werden soll, die PIN der Signaturkarte eingeben.
- **Signieren mit Zertifikatsspeicherdatei**: Wenn Sie mit dem Signaturzertifikat einer Zertifikatsspeicherdatei signieren, müssen Sie die PIN nicht erneut eingeben.

Das Ergebnis

Wenn der Governikus Signer das Erzeugen der Signaturen abgeschlossen hat, liegt folgendes Ergebnis vor:

- **PDF-Dateien**: Wenn einen PDF-Datei signiert wurde, ist das Ergebnis eine neue PDF-Datei, deren Dateinamen um den Zusatz `_signed` erweitert wurde. Beispiel: Sie haben die Datei `test.pdf` signiert. Die signierte Datei hat den Namen `test_signed.pdf`. Die originale PDF-Datei bleibt beim Signieren erhalten.
- **Andere Dateien**: Wenn eine Datei eines anderen Dateityps mit den hier angegebenen Einstellungen signiert wurde, besteht das Ergebnis aus zwei Dateien, der originalen Datei und einer neuen Datei, die die Signatur enthält. Der Dateiname der Signaturdatei besteht aus dem Dateinamen der originalen Datei und der Endung `.p7s`. Beispiel: Sie haben die Datei `test.txt` signiert. Das Ergebnis besteht aus der unveränderten Datei `test.txt` und der Signaturdatei `test.txt.p7s`. Dieses Signaturformat wird **detached** genannt. Detached bedeutet hier beigestellt.

	**Hinweis**: Wenn Sie eine detached signierte Datei beispielsweise als E-Mail-Anhang versenden, müssen Sie die originale Datei und die Signaturdatei anhängen. Nur mit der originalen Datei **und** der Signaturdatei kann die Signatur vom Empfänger geprüft werden.

2 Hardware- und Software-Voraussetzungen

Was wird für das Signieren benötigt?

Bitte beachten Sie, dass sich die folgenden Angaben mit jeder neuen Version des Governikus Signer ändern können.

- **Software Governikus Signer**: Als erstes wird natürlich ein Programm benötigt, mit dem Dateien signiert werden können. Dieser Schnelleinstieg bezieht auf den Governikus Signer ab Version 2.7.6.0.
- **Betriebssystem**: Der Governikus Signer kann auf diesen Betriebssystemen installiert werden:
  - Windows 7, 8, 8.1 und 10
  - openSUSE 13.2
  - Mac OS 10.9.x
- **Signaturzertifikat**: Ein Signaturzertifikat kann entweder als Software verfügbar sein oder als Hardware auf einer Signaturkarte. Mehr Informationen dazu finden Sie im folgenden Kapitel 3.
  - Signaturzertifikat als **Software**: In diesem Fall ist das Signaturzertifikat in einer Zertifikatsspeicherdatei enthalten. Eine Zertifikatsspeicherdatei wird auch Keystore genannt.
  - Signaturzertifikat auf **Signaturkarte**: In diesem Fall ist das Signaturzertifikat in einem Chip auf einer Signaturkarte enthalten.
- **Chipkartenleser**: Wenn Sie zum Signieren eine Signaturkarte benutzen, benötigen Sie einen Chipkartenleser. Chipkartenleser werden auch Kartenleser, Kartenlesegerät oder Chipkartenlesegerät genannt. Welche Kombinationen von Chipkartenleser, Betriebssystem und Signaturkarte für den Governikus Signer zugelassen sind, können Sie im Handbuch "Governikus Signer Systemanforderungen" nachlesen.

3 Erklärungen, Verständnis, technische Grundlagen

Signaturkarte und Zertifikatsspeicherdatei

Zum Signieren einer Datei benötigen Sie entweder eine Signaturkarte oder eine Zertifikatsspeicherdatei. Eine Zertifikatsspeicherdatei wird auch **Keystore** genannt. Beide enthalten ein Signaturzertifikat und einen privaten und einen öffentlichen Schlüssel. Beide sind vor unberechtigtem Zugriff durch eine persönliche Identifikationsnummer (PIN) geschützt. Eine Signaturkarte wird von einer Zertifizierungsstelle ausgegeben. Eine Zertifikatsspeicherdatei kann auch selbst erstellt werden. Das Signieren mit einer Signaturkarte oder mit einer Zertifikatsspeicherdatei hat rechtlich gesehen ein unterschiedliches Ergebnis:

- **Zertifikatsspeicherdatei**: Wird eine Signatur mit einer Zertifikatsspeicherdatei erstellt, so ist das Ergebnis eine fortgeschrittene elektronische Signatur.
- **Signaturkarte**: Wird eine Signatur mit einer Signaturkarte erstellt, so ist das Ergebnis eine qualifizierte elektronische Signatur (QES).

Achtung: Eine qualifizierte elektronische Signatur (QES) ist der handschriftlichen Unterschrift rechtlich gleichgestellt. Mit einer QES können Sie damit auch Verträge rechtswirksam elektronisch signieren, siehe dazu Signaturgesetz, Paragraph 6, Ziffer 2.

Wie entsteht eine elektronische Signatur?

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

1. Berechnung der Prüfsumme

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

```
0D9C3ECDFBE036E1750DE82A7863F1E6B6AC336B
```

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

2. Verschlüsselung des Hashwerts

Für die Verschlüsselung des Hashwerts wird ein so genanntes asymmetrisches Schlüsselpaar benutzt. Ein Schlüssel ist vergleichbar mit einem Kennwort. Bei der Verschlüsselung ist der Schlüssel eine Bitfolge, die einer Funktion übergeben wird. Die Funktion verschlüsselt den Hashwert mit der Bitfolge.

Ein Schlüsselpaar besteht aus einem privaten (geheimen) und einem öffentlichen Schlüssel. Das Schlüsselpaar ist auf der Signaturkarte oder der Zertifikatsspeicherdatei enthalten. Der private Schlüssel wird nie herausgegeben. Der öffentliche Schlüssel kann jedem zugänglich gemacht werden und wird hier dazu benutzt, den verschlüsselten Hashwert wieder zu entschlüsseln.

Um den Missbrauch einer Signaturkarte zu verhindern, wird vor dem Verschlüsseln mit dem privaten Schlüssel die persönliche Identifikationsnummer (PIN) abgefragt. Erst bei korrekter PIN-Eingabe wird verschlüsselt.

3.Hinzufügen des Zertifikats

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

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 Extradatei enthalten, dann heißt sie "detached", was in diesem Kontext "freistehend" bedeutet. Das Zertifikat einer Signaturkarte kann bis zur Zertifizierungsstelle nachvollzogen werden. Die Zertifizierungsstelle bestätigt auf Anfrage die Identität, womit die Authentizität nachgewiesen werden kann.

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