Elektronische Signaturen

Rechtsrahmen

- Signaturgesetz (SigG)
- Signaturverordnung (SigV)
- Bürgerliches Gesetzbuch (BGB),
  - §§ 125 ff. über die Formen von Rechtsgeschäften
- Verwaltungsverfahrensgesetz (VwVfG),
  - § 3a zur elektronischen Kommunikation und § 37 zum elektronischen Verwaltungsakt.
- weitere Rechtsvorschriften
  - 2001 durch Formanpassungsgesetz geändert wurden.
- Vorschriften der Europäischen Union.
- 1. Gesetz zur Änderung des Signaturgesetzes (1. SigÄndG)

- Einfache elektronische Signaturen
  - beispielsweise eine Unterschrift, die gescannt und als Bilddatei in eine Datei eingefügt wurde
- Fortgeschrittene elektronische Signaturen
  - beispielsweise erstellt mit einem Softwarezertifikat
- Qualifizierte elektronische Signaturen
  - erstellt mit einer Signaturkarte

Qualifizierte elektronische Signaturen mit Anbieter-Akkreditierung

- An einfache elektronische Signaturen werden keine besonderen Anforderungen gestellt
- In einem Zivilprozess unterliegen Dokumente bzw. Dateien mit einfachen elektronischen Signaturen der Beweiswürdigung durch das Gericht, das in seiner Bewertung frei ist.
- Im Rechtsstreit kommt es also darauf an, ob ein Signaturverfahren eingesetzt wurde, das vom Gericht als beweiswürdig eingestuft wird, was gegebenenfalls durch Gutachter festgestellt wird.

- Für eine fortgeschrittene elektronischen Signatur gilt nach SigG
- „Eine fortgeschrittene Signatur muss mit einem einmaligen Signaturschlüssel, der dem Signaturersteller während der Signaturerstellung zur Verfügung stehen muss, und mit Mitteln, die unter seiner alleinigen Kontrolle stehen, erstellt worden sein.
- Im Rechtsstreit werden fortgeschrittene elektronische Signaturen genauso wie „einfache“ elektronische Signaturen als Objekte des Augenscheins behandelt, d. h. die sich auf die Signatur beziehende Partei muss beweisen, dass digitale Signatur und Identifizierungsmerkmal echt sind.

Signaturen

- Nur Dokumente mit einer qualifizierten elektronischen Signatur gemäß § 2 Nr. 3 SigG können als elektronische Form eine per Gesetz geforderte Schriftform auf Papier ersetzen, vgl. § 126a BGB.

- Definition:

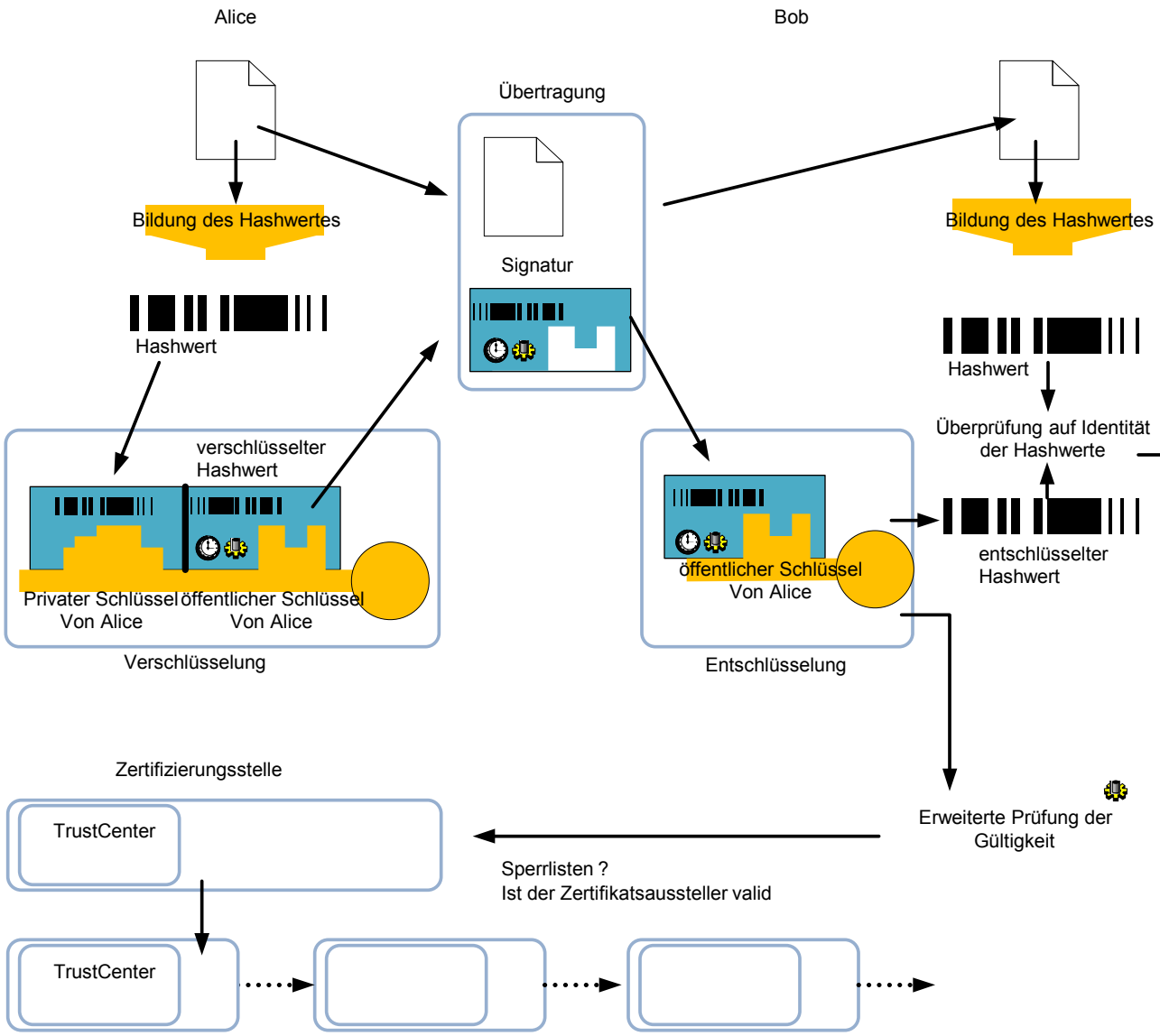
  In Übereinstimmung mit der europäischen Richtlinie ist eine qualifizierte elektronische Signatur eine fortgeschrittene elektronische Signatur, die auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruht und mit einer sicheren Signaturerstellungseinheit (SSEE) erstellt wurde. Der Signaturschlüssel darf dabei ausschließlich in der SSEE gespeichert und angewendet werden, und die Übereinstimmung der SSEE mit den Vorgaben des Signaturgesetzes muss durch eine anerkannte Stelle geprüft und bestätigt werden.

Signaturen

- Zusätzlich wird bei qualifizierten elektronischen Signaturen unterschieden, von welchem Anbieter die Zertifikate ausgestellt und die Signaturschlüssel erzeugt werden.
  - nicht-akkreditierten Anbietern
  - Anbietern mit Akkreditierung durch die Bundesnetzagentur
- Laut Signaturgesetz muss jeder Anbieter von Zertifikaten für qualifizierte elektronische Signaturen bestimmte Anforderungen bezüglich des von ihm betriebenen Rechenzentrums erfüllen.
  - Prüfung durch eine anerkannte Bestätigungsstelle (BSI oder eine private Bestätigungsstelle)
  - Bescheinigung durch die Bundesnetzagentur
  - Der Betreiber des Rechenzentrums darf sich nun als akkreditiert bezeichnen und erhält für seine Zertifizierungsdienste qualifizierte Zertifikate von der Zertifizierungsstelle der Bundesnetzagentur, die in Deutschland die Wurzelinstanz (Root CA) ist

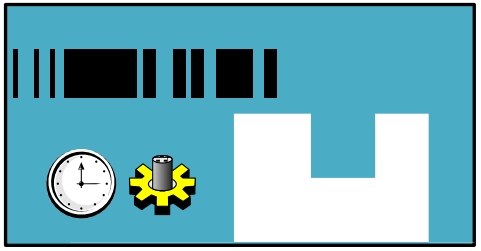
- Fortgeschrittene/qualifizierte elektronische Signaturen können technisch mit digitalen Signaturen in Verbindung mit digitalen Zertifikaten von einer Public-Key-Infrastruktur (PKI) realisiert werden.
- Bei diesen Verfahren wird ein Schlüsselpaar verwendet. Ein Schlüssel wird für die Erzeugung der Signatur verwendet (Signaturschlüssel) und ein Schlüssel für die Prüfung (Signaturprüfschlüssel). Bei qualifizierten Signaturen ist die Zuordnung der asymmetrischen Schlüsselpaare gemäß deutschem Signaturgesetz zwingend erforderlich.
- Innerhalb der PKI gibt es ein hierarchisches System zur Vertrauensstellung

Signaturen



- ✓Inhalt
- ✓Unterzeichner
- ✓Zeitpunkt der Unterzeichnung
- ✓Herausgeber des Zertifikates

Elemente einer Signatur



- Verschlüsselter Hashwert
- Verschlüsselungszeitpunkt
- Zertifikat mit öffentlichem Schlüssel
- Herausgeber des Zertifikates

Notwendige Komponenten

- Zertifikat
  - Bescheinigung, dass die Signatur- und Prüfschlüssel einer Person zugeordnet wurden und die Identität der Person bestätigt wird (Signaturkarte)
- Hardware (Kartenleser)
- Software

Zertifikatsanbieter

Quelle: Bundesnetzagentur

- TELESEC (Telekom)
- DTrust (Bundesdruckerei)
- SignTrust (Deutsche Post)
- STrust (Sparkassen)

Hardware

Leserklassen

- Mind. Klasse 2 Leser
  - ReinerSCT
  - Kobil
  - Gemalto

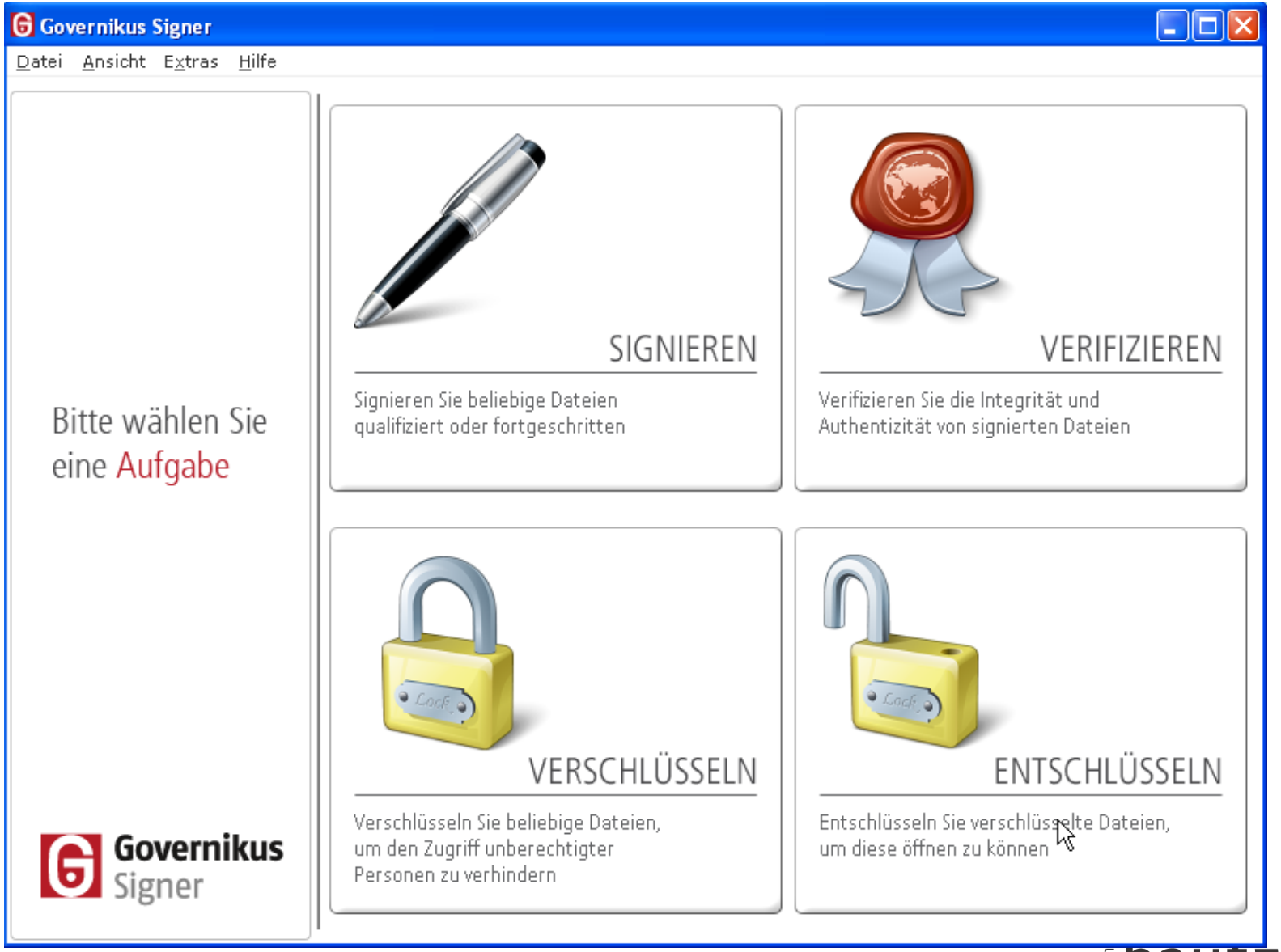
Software

- BOS Bremen (GovernikusSigner)

  Ist Bestandteil der EGov-Basiskomponenten des Freistaates

- Seccomerce
- OpenLimit (ccSigner)
- .. Liste bei der Netzagentur

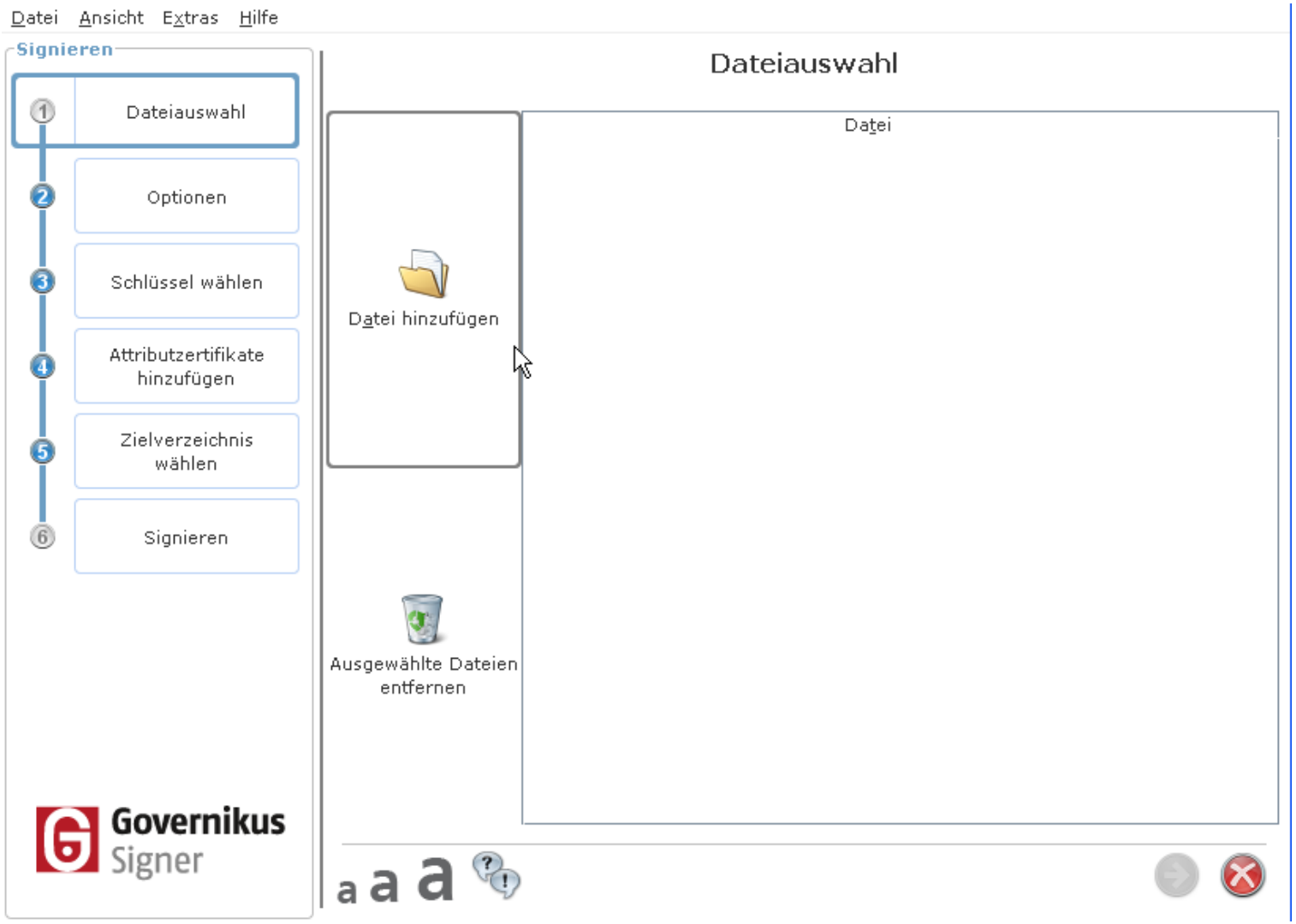
Signaturen


Governikus Signer
Datei Ansicht Extras Hilfe
Bitte wählen Sie eine Aufgabe
Governikus Signer
SIGNIEREN
Signieren Sie beliebige Dateien qualifiziert oder fortgeschritten
VERIFIZIEREN
Verifizieren Sie die Integrität und Authentizität von signierten Dateien
VERSCHLÜSSELN
Verschlüsseln Sie beliebige Dateien, um den Zugriff unberechtigter Personen zu verhindern
ENTSCHLÜSSELN
Entschlüsseln Sie verschlüsselte Dateien, um diese öffnen zu können

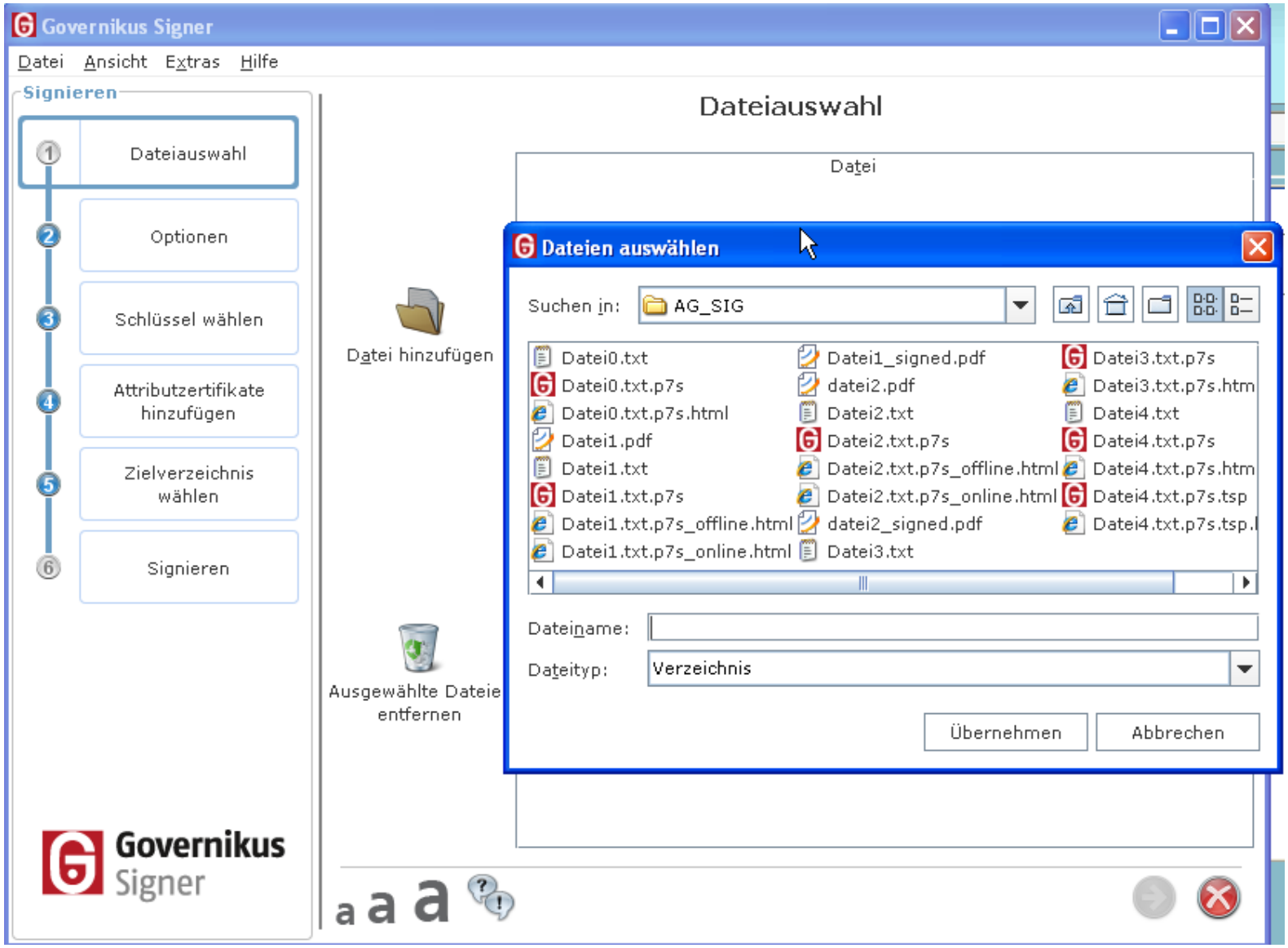
Signaturen


SIGNIEREN
Signieren Sie beliebige Dateien
qualifiziert oder fortgeschritten

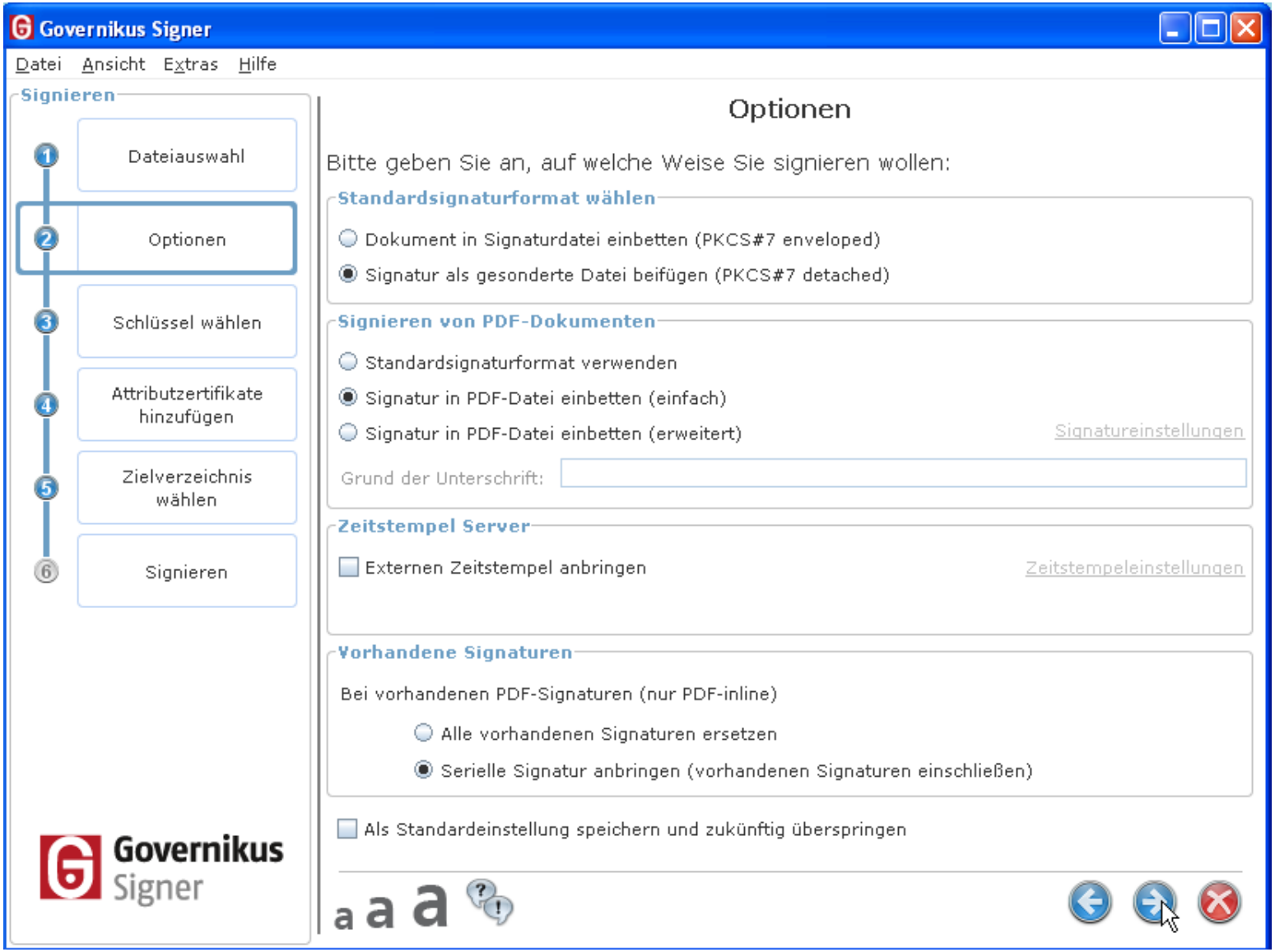
Signaturen


Datei Ansicht Extras Hilfe
Signieren
1 Dateiauswahl
2 Optionen
3 Schlüssel wählen
4 Attributzertifikate hinzufügen
5 Zielverzeichnis wählen
6 Signieren
Governikus Signer
Dateiauswahl
Datei
Datei hinzufügen
Ausgewählte Dateien entfernen
a a a

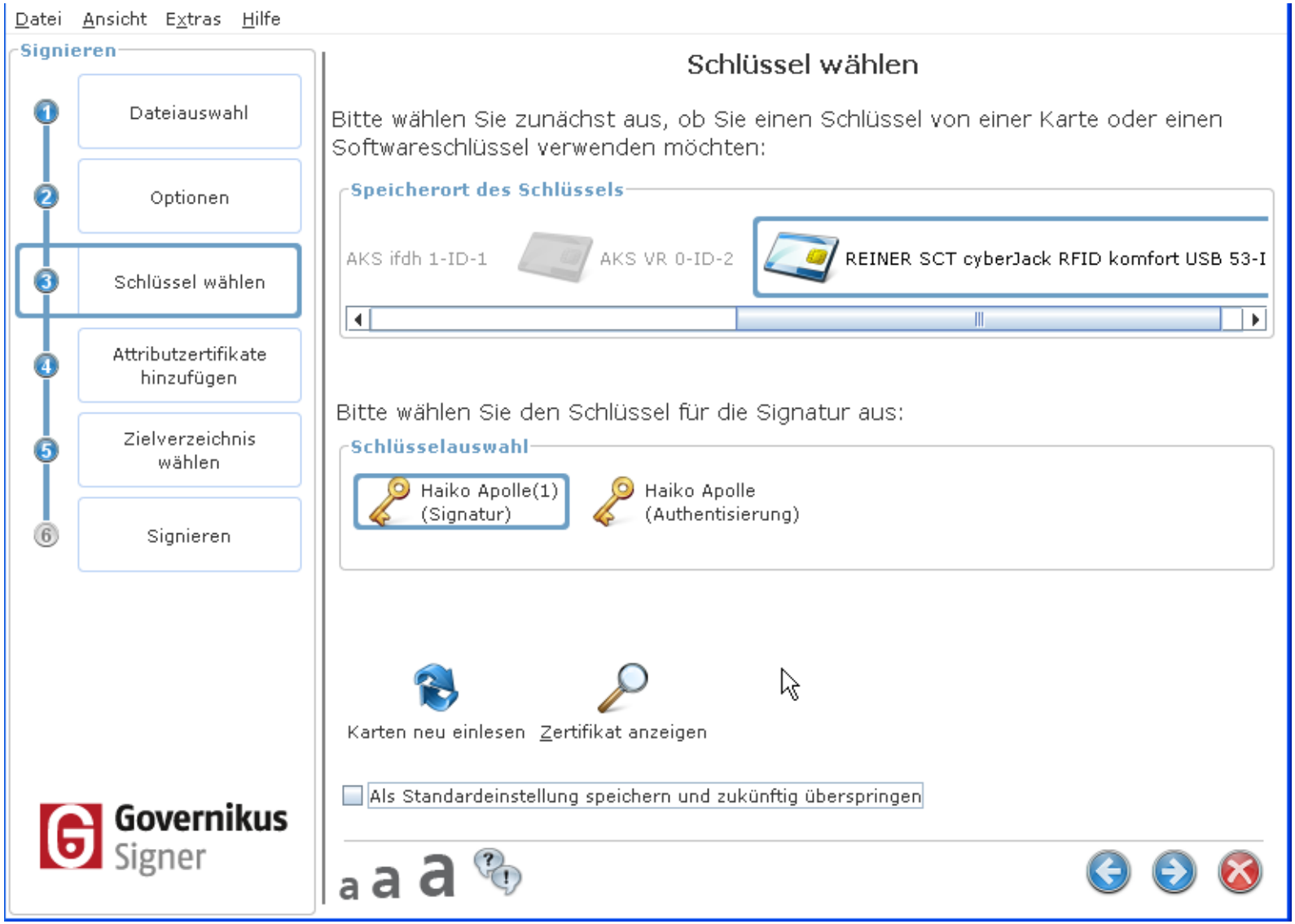
Signaturen


Governikus Signer
Datei Ansicht Extras Hilfe
Signieren
1 Dateiauswahl
2 Optionen
3 Schlüssel wählen
4 Attributzertifikate hinzufügen
5 Zielverzeichnis wählen
6 Signieren
Governikus Signer
Dateiauswahl
Datei
Datei hinzufügen
Ausgewählte Dateie entfernen
Dateien auswählen
Suchen in: AG_SIG
Datei0.txt
Datei0.txt.p7s
Datei0.txt.p7s.html
Datei1.pdf
Datei1.txt
Datei1.txt.p7s
Datei1.txt.p7s_offline.html
Datei1.txt.p7s_online.html
Datei1_signed.pdf
datei2.pdf
Datei2.txt
Datei2.txt.p7s
Datei2.txt.p7s_offline.html
Datei2.txt.p7s_online.html
datei2_signed.pdf
Datei3.txt
Datei3.txt.p7s
Datei3.txt.p7s.htm
Datei4.txt
Datei4.txt.p7s
Datei4.txt.p7s.htm
Datei4.txt.p7s.tsp
Dateiname:
Dateityp: Verzeichnis
Übernehmen
Abbrechen

Signaturen


Governikus Signer
Datei Ansicht Extras Hilfe
Signieren
1 Dateiauswahl
2 Optionen
3 Schlüssel wählen
4 Attributzertifikate hinzufügen
5 Zielverzeichnis wählen
6 Signieren
Governikus Signer
Optionen
Bitte geben Sie an, auf welche Weise Sie signieren wollen:
Standardsignaturformat wählen
Dokument in Signaturdatei einbetten (PKCS#7 enveloped)
Signatur als gesonderte Datei beifügen (PKCS#7 detached)
Signieren von PDF-Dokumenten
Standardsignaturformat verwenden
Signatur in PDF-Datei einbetten (einfach)
Signatur in PDF-Datei einbetten (erweitert)
Signatureinstellungen
Grund der Unterschrift:
Zeitstempel Server
Externen Zeitstempel anbringen
Zeitstempeleinstellungen
Vorhandene Signaturen
Bei vorhandenen PDF-Signaturen (nur PDF-inline)
Alle vorhandenen Signaturen ersetzen
Serielle Signatur anbringen (vorhandenen Signaturen einschließen)
Als Standardeinstellung speichern und zukünftig überspringen

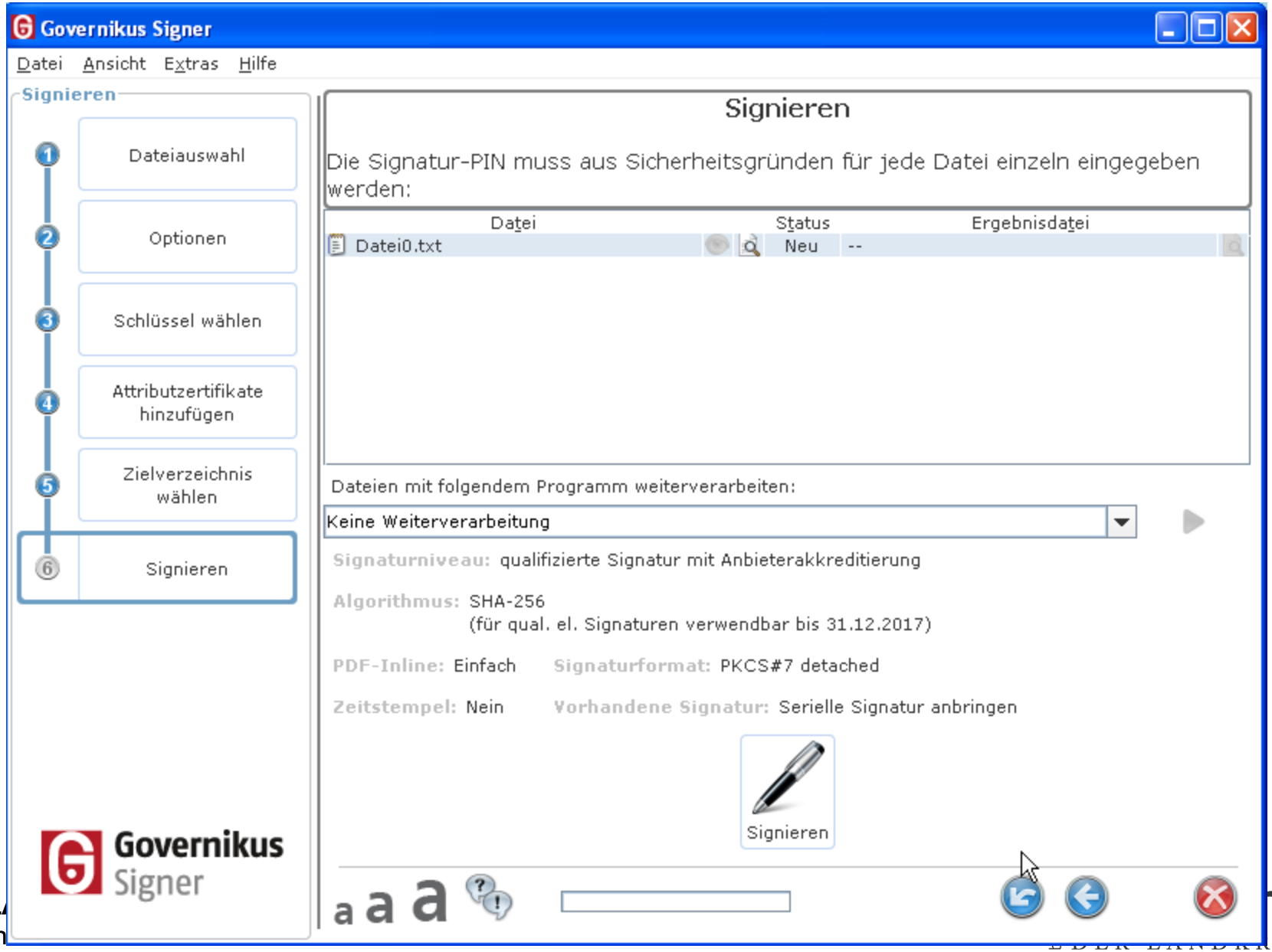
Signaturen


Datei Ansicht Extras Hilfe
Signieren
1 Dateiauswahl
2 Optionen
3 Schlüssel wählen
4 Attributzertifikate hinzufügen
5 Zielverzeichnis wählen
6 Signieren
Governikus Signer
Schlüssel wählen
Bitte wählen Sie zunächst aus, ob Sie einen Schlüssel von einer Karte oder einen Softwareschlüssel verwenden möchten:
Speicherort des Schlüssels
AKS ifdh 1-ID-1
AKS VR 0-ID-2
REINER SCT cyberJack RFID komfort USB 53-I
Bitte wählen Sie den Schlüssel für die Signatur aus:
Schlüsselauswahl
Haiko Apolle(1) (Signatur)
Haiko Apolle (Authentisierung)
Karten neu einlesen
Zertifikat anzeigen
Als Standardeinstellung speichern und zukünftig überspringen

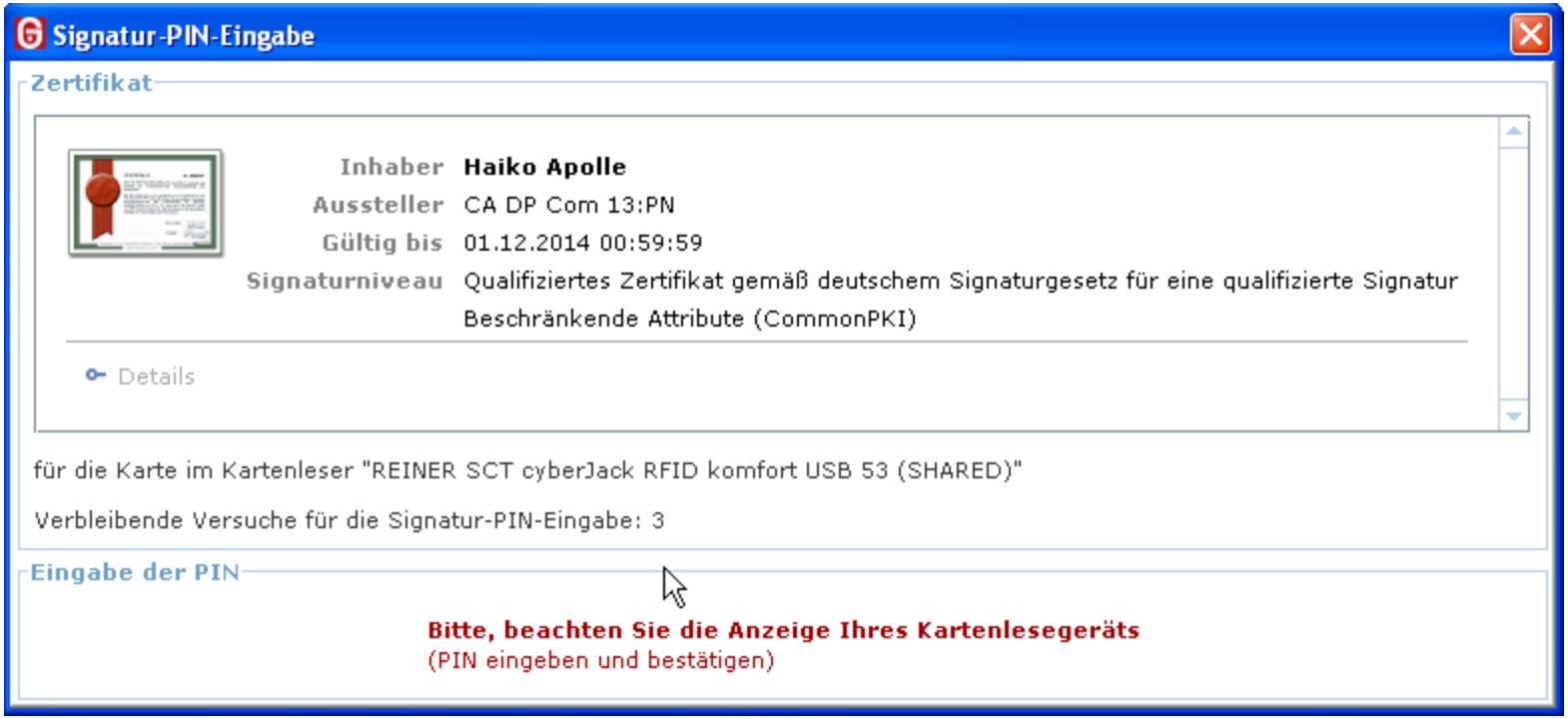
Signaturen


Datei Ansicht Extras Hilfe
Signieren
1 Dateiauswahl
2 Optionen
3 Schlüssel wählen
4 Attributzertifikate hinzufügen
5 Zielverzeichnis wählen
6 Signieren
Governikus Signer
Zielverzeichnis wählen
Zielverzeichnis wählen
Quellverzeichnis nutzen
Zielverzeichnis wählen
Als Standardeinstellung speichern und zukünftig überspringen

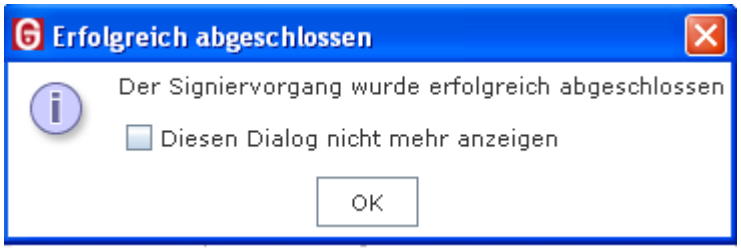
Signaturen


Governikus Signer
Datei Ansicht Extras Hilfe
Signieren
1 Dateiauswahl
2 Optionen
3 Schlüssel wählen
4 Attributzertifikate hinzufügen
5 Zielverzeichnis wählen
6 Signieren
Governikus Signer
Signieren
Die Signatur-PIN muss aus Sicherheitsgründen für jede Datei einzeln eingegeben werden:
Datei
Status
Ergebnisdatei
Datei0.txt
Neu
--
Dateien mit folgendem Programm weiterverarbeiten:
Keine Weiterverarbeitung
Signaturniveau: qualifizierte Signatur mit Anbieterakkreditierung
Algorithmus: SHA-256
(für qual. el. Signaturen verwendbar bis 31.12.2017)
PDF-Inline: Einfach
Signaturformat: PKCS#7 detached
Zeitstempel: Nein
Vorhandene Signatur: Serielle Signatur anbringen
Signieren

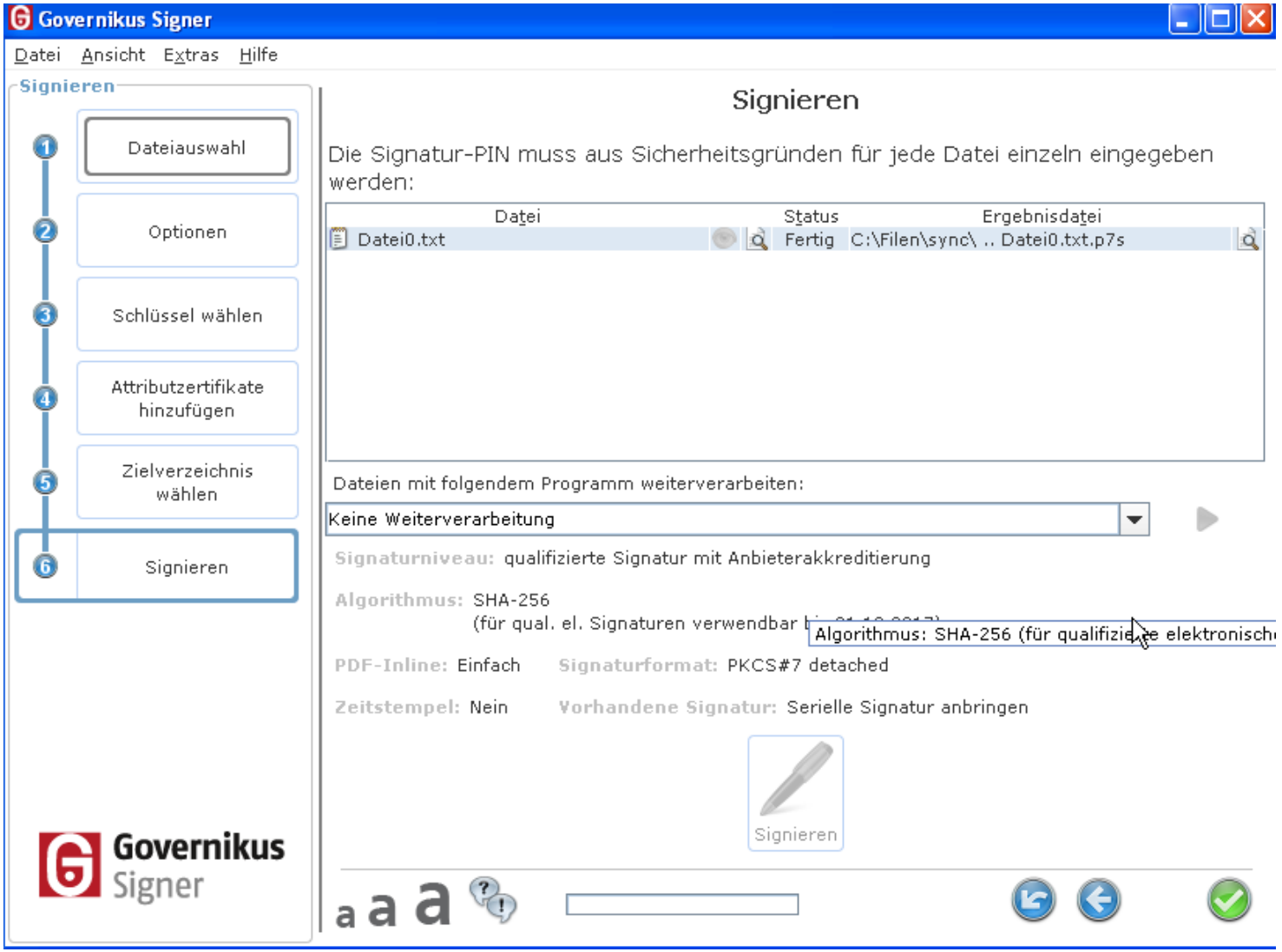
Signaturen


Signatur-PIN-Eingabe
Zertifikat
Inhaber Haiko Apolle
Aussteller CA DP Com 13:PN
Gültig bis 01.12.2014 00:59:59
Signaturniveau Qualifiziertes Zertifikat gemäß deutschem Signaturgesetz für eine qualifizierte Signatur
Beschränkende Attribute (CommonPKI)
Details
für die Karte im Kartenleser "REINER SCT cyberJack RFID komfort USB 53 (SHARED)"
Verbleibende Versuche für die Signatur-PIN-Eingabe: 3
Eingabe der PIN
Bitte, beachten Sie die Anzeige Ihres Kartenlesegeräts
(PIN eingeben und bestätigen)

Signaturen


Erfolgreich abgeschlossen
Der Signiervorgang wurde erfolgreich abgeschlossen
Diesen Dialog nicht mehr anzeigen
OK

Signaturen

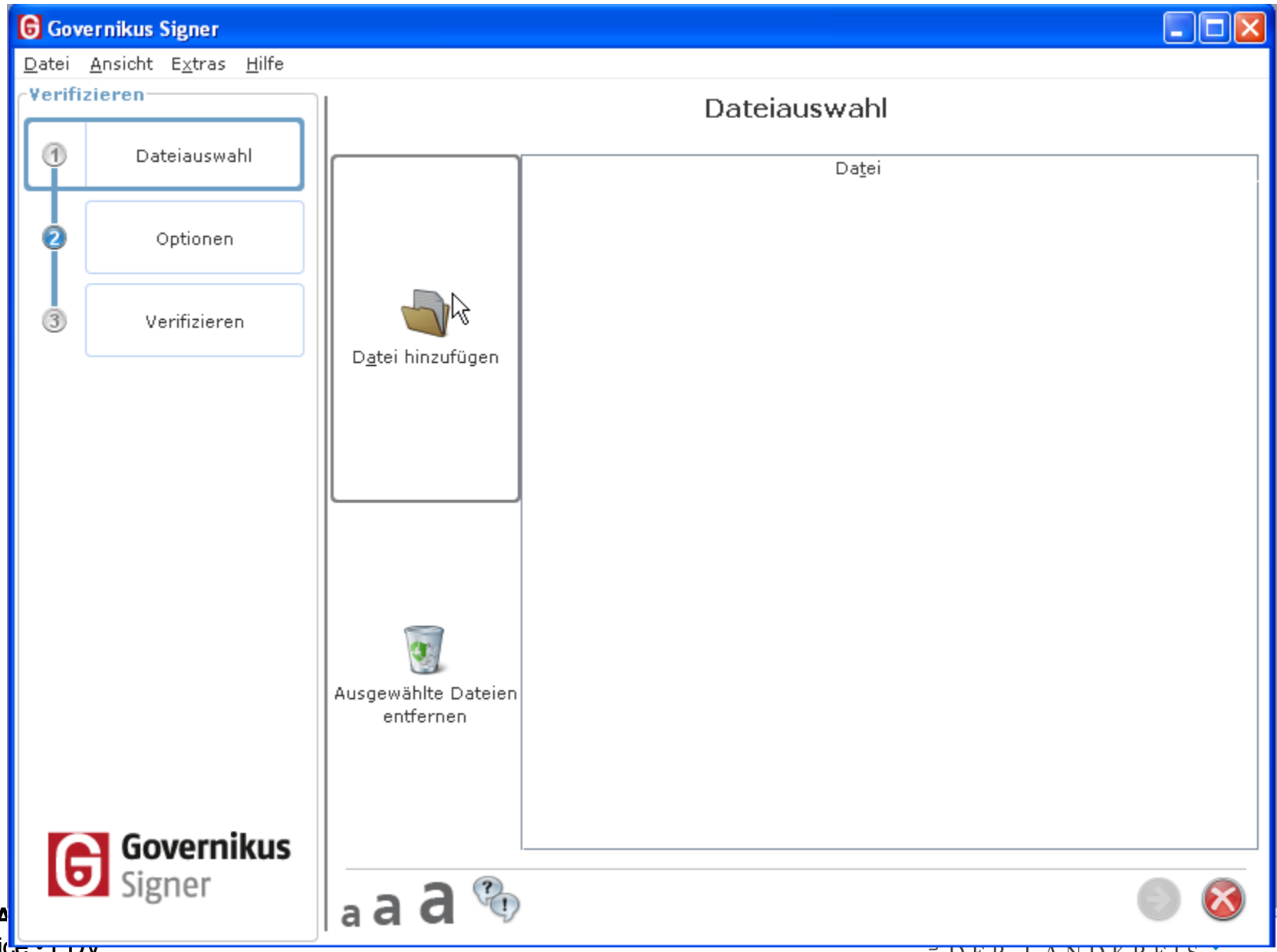

Governikus Signer
Datei Ansicht Extras Hilfe
Signieren
1 Dateiauswahl
2 Optionen
3 Schlüssel wählen
4 Attributzertifikate hinzufügen
5 Zielverzeichnis wählen
6 Signieren
Governikus Signer
Signieren
Die Signatur-PIN muss aus Sicherheitsgründen für jede Datei einzeln eingegeben werden:
Datei
Status
Ergebnisdatei
Datei0.txt
Fertig
C:\Filen\sync\ .. Datei0.txt.p7s
Dateien mit folgendem Programm weiterverarbeiten:
Keine Weiterverarbeitung
Signaturniveau: qualifizierte Signatur mit Anbieterakkreditierung
Algorithmus: SHA-256
(für qual. el. Signaturen verwendbar
Algorithmus: SHA-256 (für qualifizierte elektronische
PDF-Inline: Einfach
Signaturformat: PKCS#7 detached
Zeitstempel: Nein
Vorhandene Signatur: Serielle Signatur anbringen
Signieren

- **Live**
  - **Signieren eines Dokumentes**

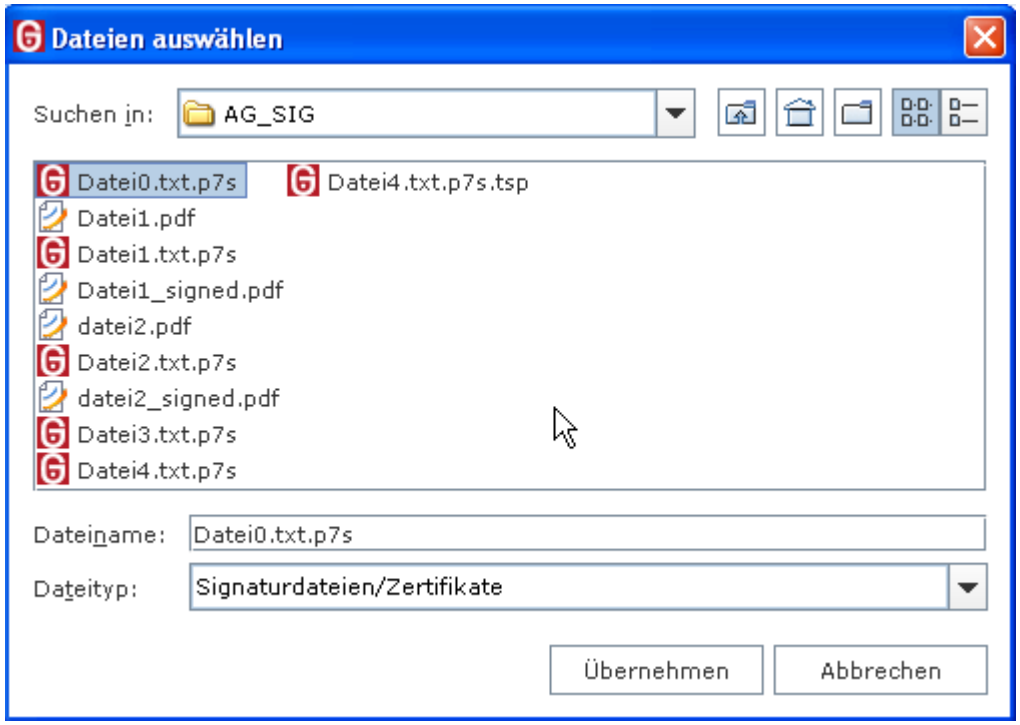
Signaturen


VERIFIZIEREN
Verifizieren Sie die Integrität und
Authentizität von signierten Dateien

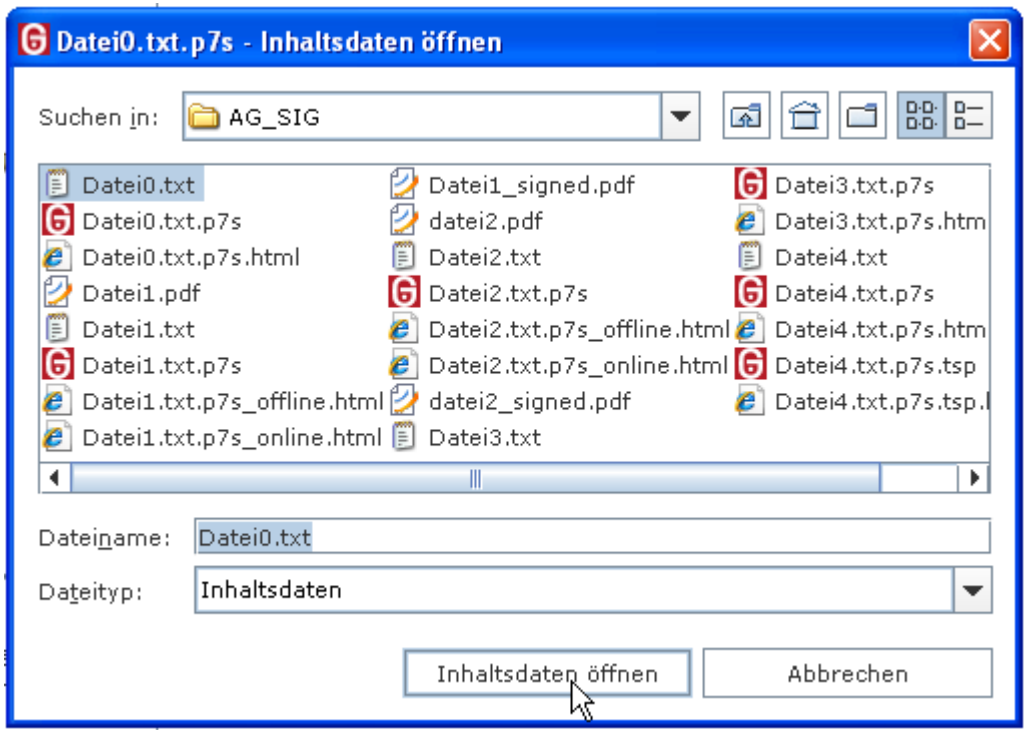
Signaturen


Governikus Signer
Datei Ansicht Extras Hilfe
Verifizieren
1 Dateiauswahl
2 Optionen
3 Verifizieren
Governikus Signer
Dateiauswahl
Datei hinzufügen
Ausgewählte Dateien entfernen
Datei

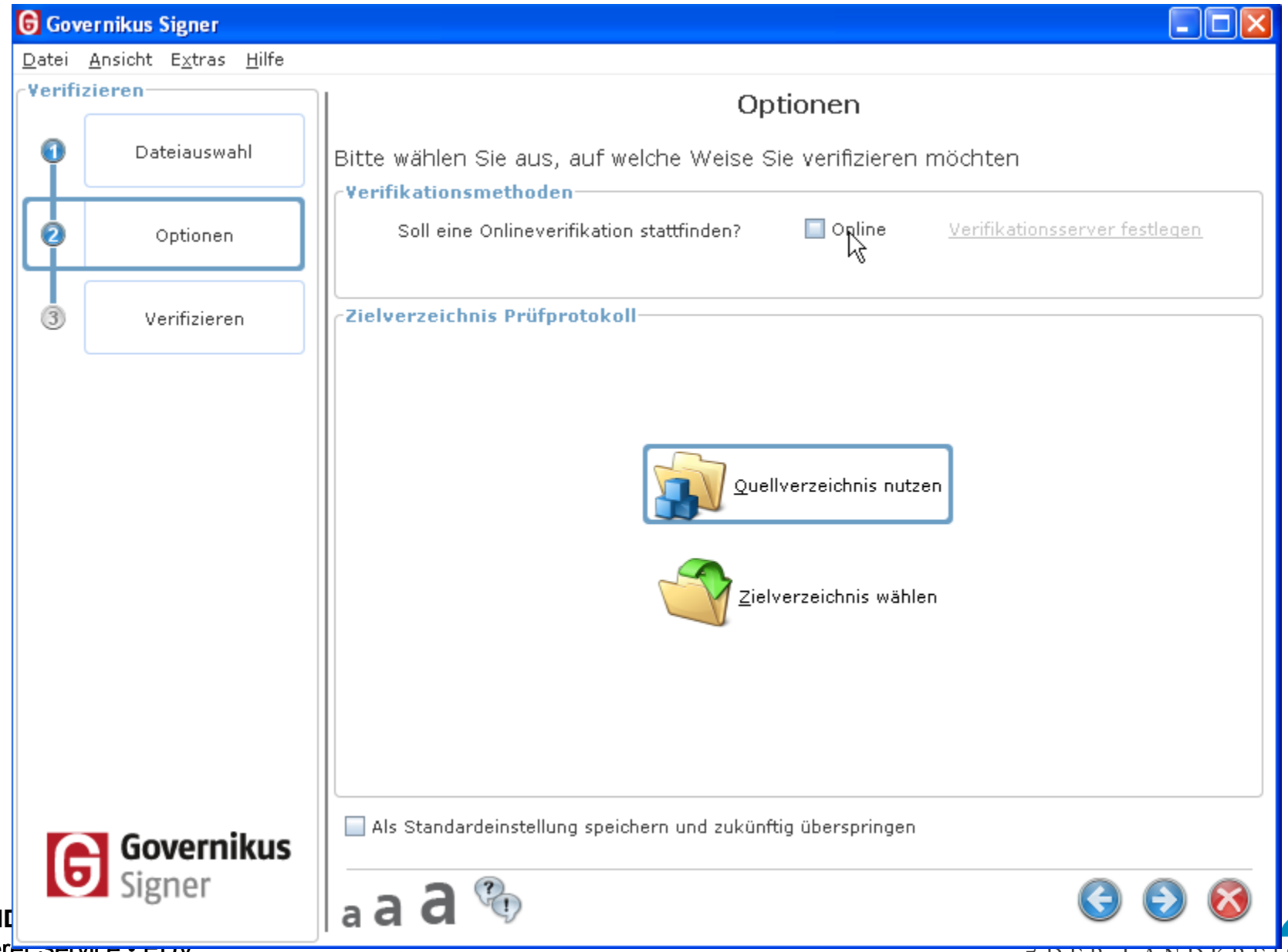
Signaturen


Dateien auswählen
Suchen in:
AG_SIG
Datei0.txt.p7s
Datei4.txt.p7s.tsp
Datei1.pdf
Datei1.txt.p7s
Datei1_signed.pdf
datei2.pdf
Datei2.txt.p7s
datei2_signed.pdf
Datei3.txt.p7s
Datei4.txt.p7s
Dateiname:
Datei0.txt.p7s
Dateityp:
Signaturdateien/Zertifikate
Übernehmen
Abbrechen

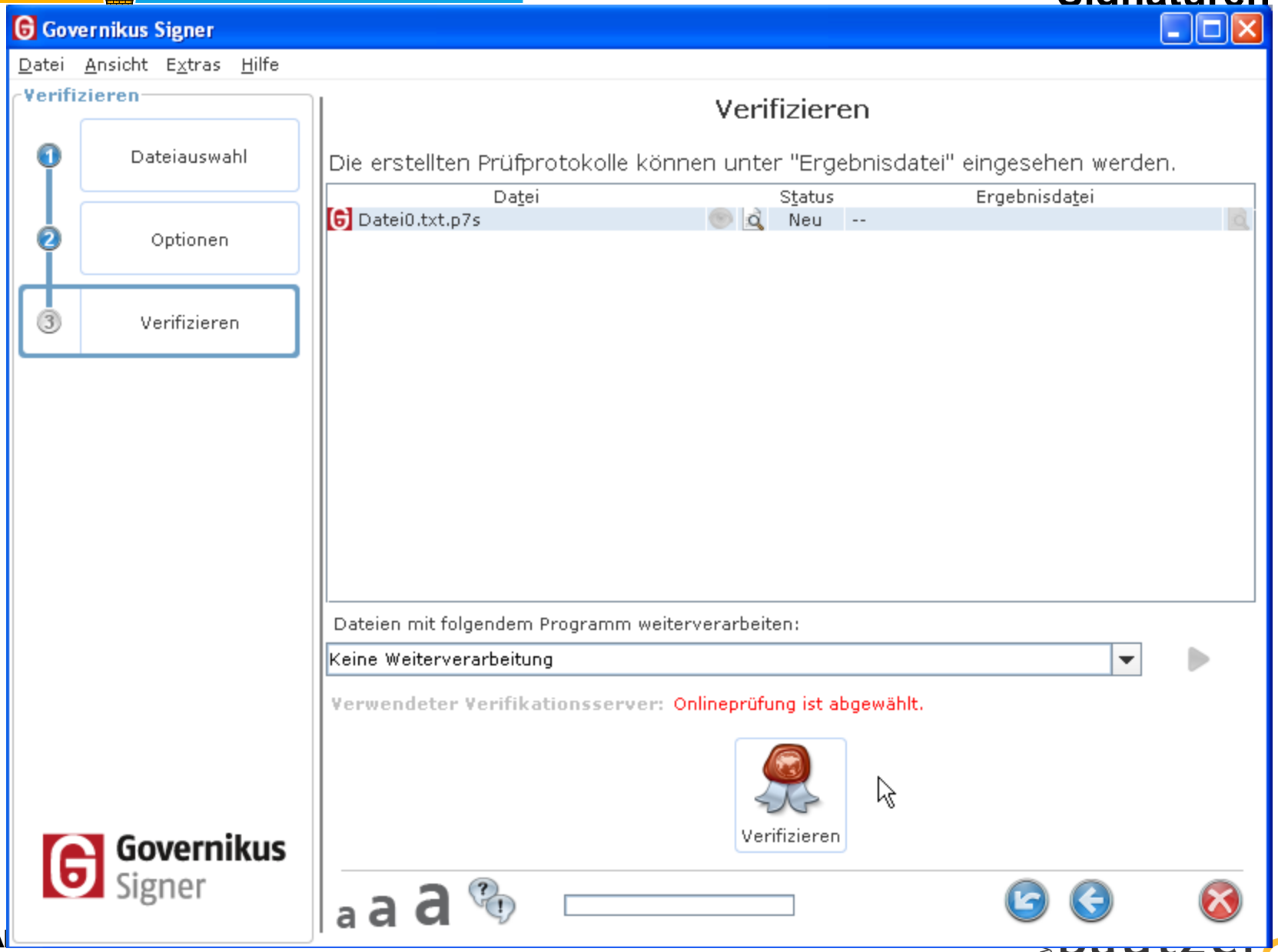
Signaturen


Datei0.txt.p7s - Inhaltsdaten öffnen
Suchen in:
AG_SIG
Datei0.txt
Datei0.txt.p7s
Datei0.txt.p7s.html
Datei1.pdf
Datei1.txt
Datei1.txt.p7s
Datei1.txt.p7s_offline.html
Datei1.txt.p7s_online.html
Datei1_signed.pdf
datei2.pdf
Datei2.txt
Datei2.txt.p7s
Datei2.txt.p7s_offline.html
Datei2.txt.p7s_online.html
datei2_signed.pdf
Datei3.txt
Datei3.txt.p7s
Datei3.txt.p7s.htm
Datei4.txt
Datei4.txt.p7s
Datei4.txt.p7s.htm
Datei4.txt.p7s.tsp
Dateiname:
Datei0.txt
Dateityp:
Inhaltsdaten
Inhaltsdaten öffnen
Abbrechen

Signaturen

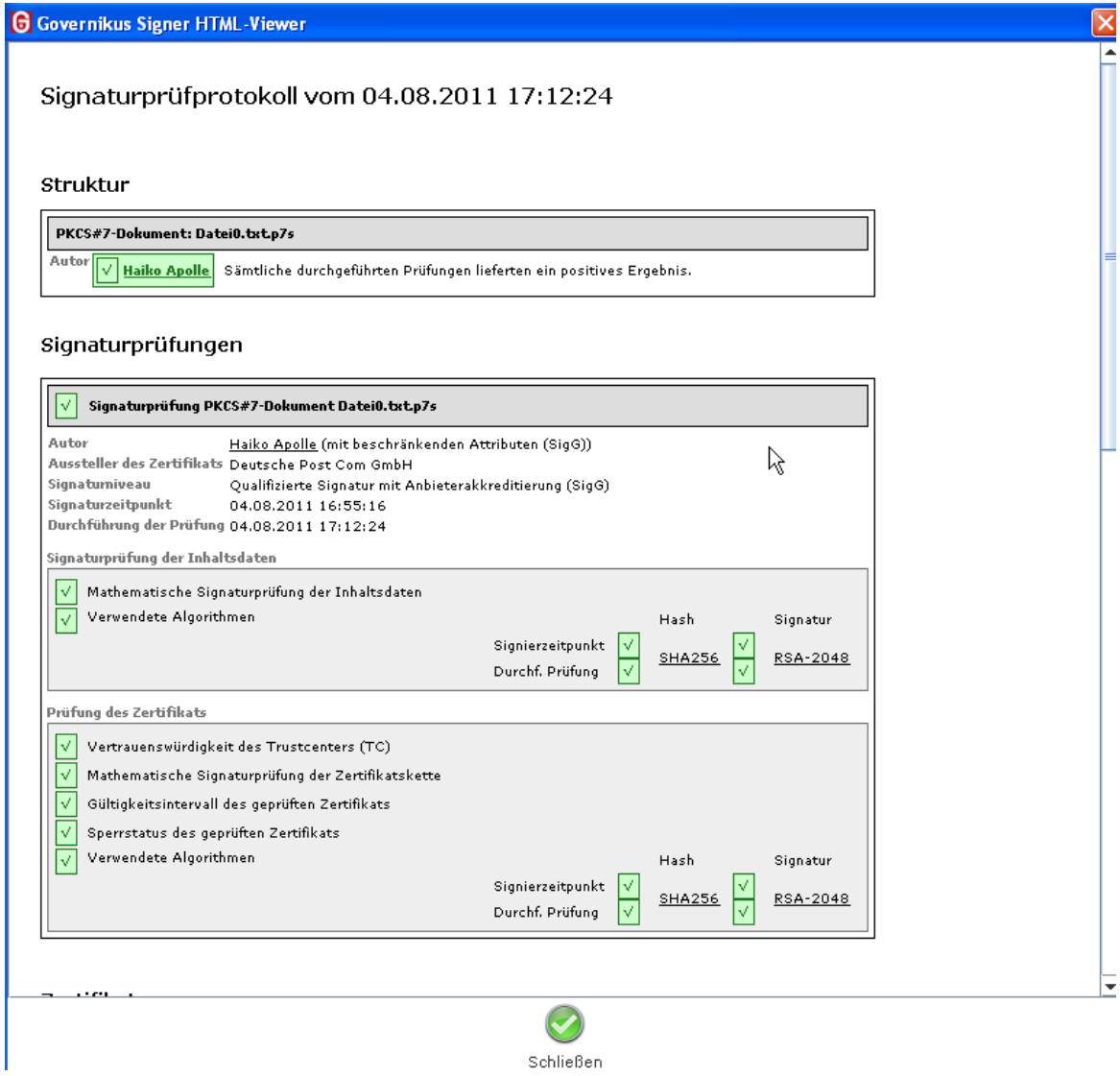

Governikus Signer
Datei Ansicht Extras Hilfe
Verifizieren
1 Dateiauswahl
2 Optionen
3 Verifizieren
Governikus Signer
Optionen
Bitte wählen Sie aus, auf welche Weise Sie verifizieren möchten
Verifikationsmethoden
Soll eine Onlineverifikation stattfinden?
Online
Verifikationsserver festlegen
Zielverzeichnis Prüfprotokoll
Quellverzeichnis nutzen
Zielverzeichnis wählen
Als Standardeinstellung speichern und zukünftig überspringen

Signaturen


Governikus Signer
Datei Ansicht Extras Hilfe
Verifizieren
1 Dateiauswahl
2 Optionen
3 Verifizieren
Governikus Signer
Verifizieren
Die erstellten Prüfprotokolle können unter "Ergebnisdatei" eingesehen werden.
Datei
Status
Ergebnisdatei
Datei0.txt.p7s
Neu
--
Dateien mit folgendem Programm weiterverarbeiten:
Keine Weiterverarbeitung
Verwendeter Verifikationsserver: Onlineprüfung ist abgewählt.
Verifizieren

Signaturen

Signaturen


Governikus Signer HTML-Viewer
Signaturprüfprotokoll vom 04.08.2011 17:12:24
Struktur
PKCS#7-Dokument: Datei0.txt.p7s
Autor
Haiko Apolle
Sämtliche durchgeführten Prüfungen lieferten ein positives Ergebnis.
Signaturprüfungen
Signaturprüfung PKCS#7-Dokument Datei0.txt.p7s
Autor
Haiko Apolle (mit beschränkenden Attributen (SigG))
Aussteller des Zertifikats
Deutsche Post Com GmbH
Signaturniveau
Qualifizierte Signatur mit Anbieterakkreditierung (SigG)
Signaturzeitpunkt
04.08.2011 16:55:16
Durchführung der Prüfung
04.08.2011 17:12:24
Signaturprüfung der Inhaltsdaten
Mathematische Signaturprüfung der Inhaltsdaten
Verwendete Algorithmen
Hash
Signatur
Signierzeitpunkt
Durchf. Prüfung
SHA256
RSA-2048
Prüfung des Zertifikats
Vertrauenswürdigkeit des Trustcenters (TC)
Mathematische Signaturprüfung der Zertifikatskette
Gültigkeitsintervall des geprüften Zertifikats
Sperrstatus des geprüften Zertifikats
Verwendete Algorithmen
Hash
Signatur
Signierzeitpunkt
Durchf. Prüfung
SHA256
RSA-2048
Schließen

Signaturen

- **Live**
  - **-Überprüfen der Signatur eines Dokumentes**

Zusammenfassung

- rechtliche Grundlagen existieren
- technische Grundlagen verfügbar
- Organisatorische Regelungen für den Einsatz notwendig

Offene Fragen

-Wer darf signieren?

-Wo soll signiert werden?

-Was soll signiert werden?

-Was wollen wir eingangsseitig zulassen?

Zielstellung

Bis IV/2011 werden die organisatorischen Vorraussetzungen für den Einsatz der QES in allen Strukturen des Landratsamtes geschaffen

Vielen Dank für Ihre Aufmerksamkeit