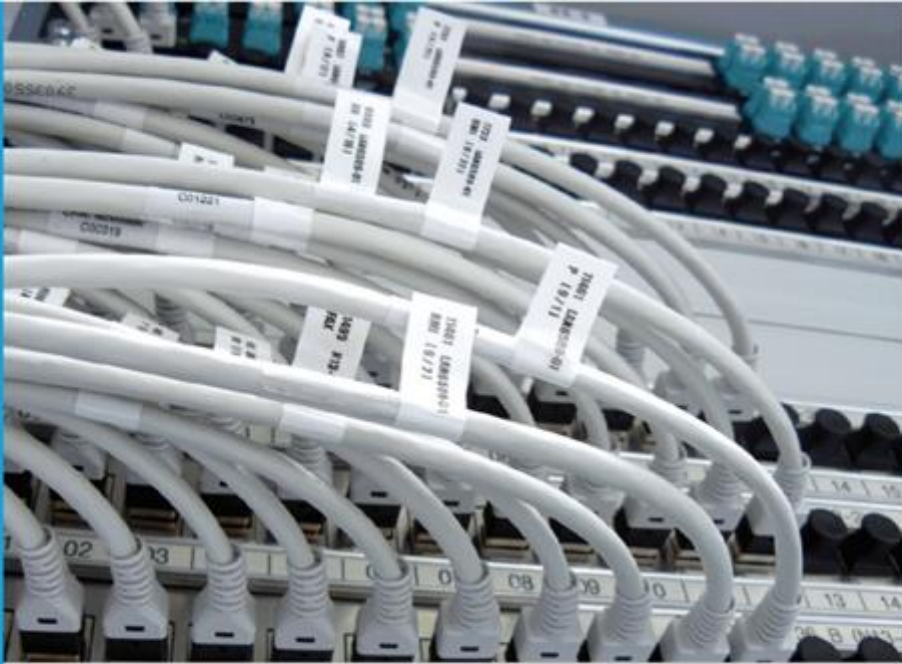




IT-Dienstleistungszentrum des Freistaats Bayern



- READY
- ALARM
- MESSAGE

Dokumentation

Signaturprüfung

Bearbeitung:
Erich Lechner

München, den 13.02.2017

Dokumententwicklung

Version	Datum	Bearbeiter	Beschreibung, QS-Maßnahme	Status *s. u.
1.0	13.02.2017	Erich Lechner	Dokumentation der Web-anwendung Signaturprüfung	freigegeben

Inhaltsverzeichnis

<u>Kapitel</u>	<u>Thema</u>	<u>Seite</u>
1	Funktionalität	4
2	Bedienung	5
2.1	Prüfung einer Datei mit eingebetteter Signatur	6
2.2	Prüfung einer oder mehrerer Dateien mit eingebetteter oder separater Signatur	6
3	Ergebnisse	7
4	Prüfprotokoll	8
5.	Grundlagen	9
5.1	Elektronische Signatur	9
5.2	Signierte Datei	10
5.3	Verifizierung	11
5.4	Zertifikatsprüfung	11

1 Funktionalität

Mit dem Signaturprüfer können Sie elektronische Dokumente, welche mit einer Signatur versehen sind, auf ihre Gültigkeit prüfen. Die Signatur einer Datei ist entweder Teil dieser Datei (typischerweise PDF) oder sie wird in einer separaten Datei mitgeliefert. Die Prüfung umfasst

- eine mathematische Analyse der Signatur, d.h. ob die Signatur dem Inhalt der Datei entspricht
- eine Prüfung des(der) Zertifikat(e) der Signatur auf ihre Gültigkeit

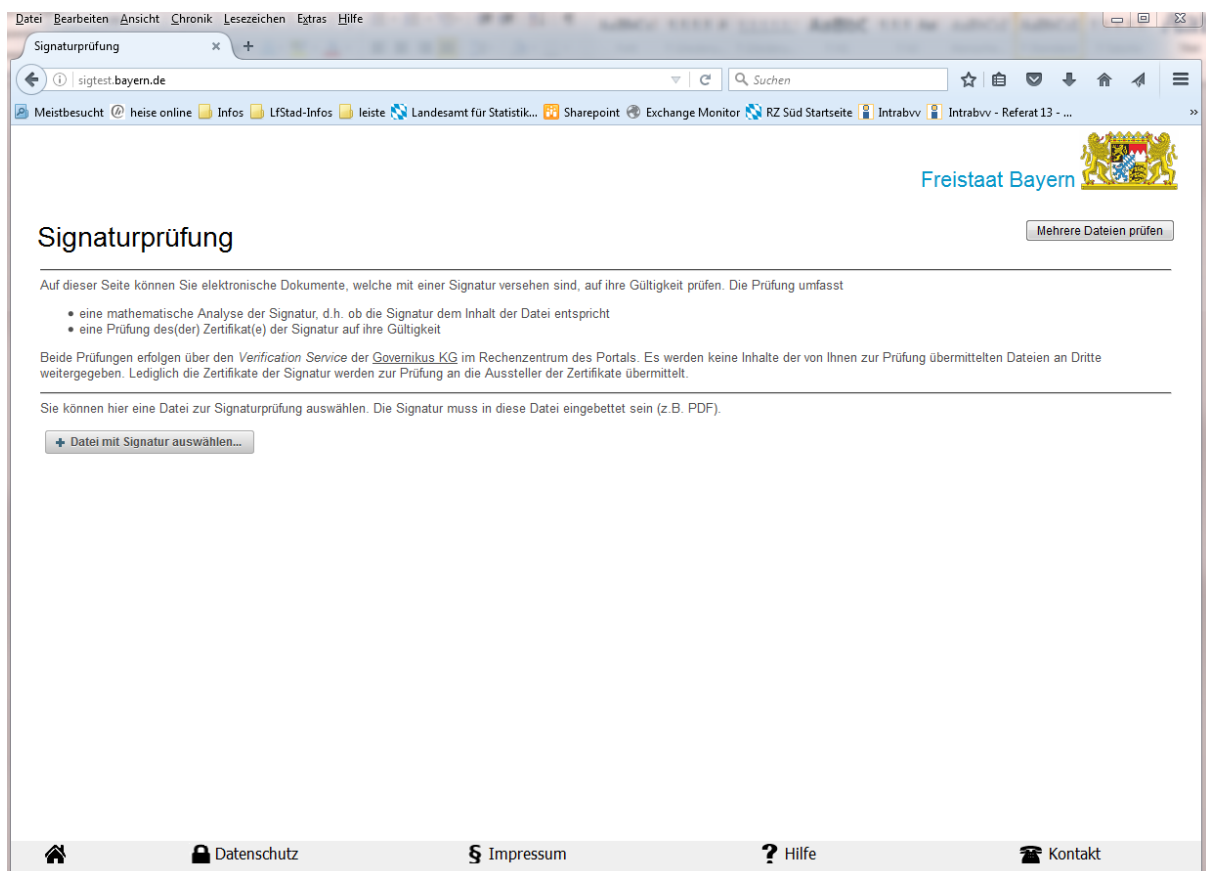
Beide Prüfungen erfolgen über den Verification Service der Governikus KG im Rechenzentrum des Portals. Es werden keine Inhalte der von Ihnen zur Prüfung übermittelten Dateien an Dritte weitergegeben. Lediglich die Zertifikate der Signatur werden zur Prüfung an die Aussteller der Zertifikate übermittelt.

2 Bedienung

Der Aufruf des Signaturprüfers ist nur aus dem Behördennetz möglich und erfolgt über den Link:

<http://sigtest.bayern.de>

Die Benutzeroberfläche des Signaturprüfers gliedert sich in eine Titelzeile, das Anwendungsfenster und eine Fußzeile. In der Titelzeile ist auf der rechten Seite immer eine Schaltfläche eingeblendet, mit der Sie die für die aktuelle Ansicht gültige Aktion durchführen können, Ein Klick auf den Titel links bringt Sie immer auf die Hauptseite zurück. Die Fußzeile enthält neben der Schaltfläche um auf die Hauptseite zu kommen Links zu den wichtigen Informationen zu dieser Anwendung. Im zentralen Anwendungsfenster können Sie Dateien zur Prüfung der Signatur auswählen und die Ergebnisse einsehen.



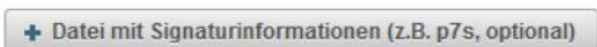
2.1 Prüfung einer Datei mit eingebetteter Signatur

Wenn Sie nur eine Datei mit eingebetteter Signatur prüfen möchten, so können Sie dies in dieser Ansicht machen. Wählen Sie die Datei über die Schaltfläche 'Datei mit Signatur auswählen...' aus oder - falls Ihr Browser dies unterstützt - ziehen Sie die Datei mit der Maus auf diese Schaltfläche. Die Prüfung der Signatur erfolgt danach sofort.

+ Datei mit Signatur auswählen...

2.2 Prüfung einer oder mehrerer Dateien mit eingebetteter oder separater Signatur

Wenn Sie mehrere Dateien oder Dateien mit separater Signaturdatei prüfen möchten, müssen Sie über die Schaltfläche 'Mehrere Dateien prüfen' in diese Ansicht wechseln. Hier können Sie über die Schaltflächen 'Signierte Datei' und 'Datei mit Signaturinformationen' die entsprechenden Dateien auswählen oder - falls Ihr Browser dies unterstützt - die Datei mit der Maus auf die entsprechende Schaltfläche ziehen. Mit den Schaltflächen 'Löschen' oder 'Hinzufügen' auf der linken Seite können Sie entweder einzelne Zeilen wieder entfernen oder eine neue Zeile für weitere Dateien hinzufügen.

	Signierte Datei TestDatei_signed_A.pdf		+ Datei mit Signaturinformationen (z.B. p7s, optional)
	Signierte Datei TestDatei.pdf		Datei mit Signaturinformationen (z.B. p7s, optional) TestDatei.pdf.p7s
			

Die Prüfung wird über die Schaltfläche 'Signaturprüfung durchführen' rechts oben gestartet.


Signaturprüfung

Signaturprüfung durchführen


3 Ergebnisse

Das Ergebnis - oder bei mehreren Dateien die Ergebnisse - der Prüfung werden in einer Übersicht dargestellt. Diese Übersicht gliedert sich in


- Der Name der Datei, ggf. der Name der Datei mit der separaten Signatur.
- Die Meldungen der Prüfung.
- Die Signaturen, mit der die Datei signiert war. Für jede Signatur wird der Inhaber des Zertifikats, der Zeitpunkt der Signatur sowie der Status des Zertifikats zu diesem Zeitpunkt angegeben.

 **TestDatei_signed_A.pdf**

Meldungen

 Sämtliche durchgeführten Prüfungen lieferten ein positives Ergebnis.

Signaturen

Zertifikat	Zeitpunkt der Signatur	Status des Zertifikats zum Zeitpunkt der Signatur
Name	Heute	 VALID

[Prüfergebnis als PDF](#) [Governikus Resultat](#)

 **TestDatei.pdf (Signatur in TestDatei.pdf.p7s)**

Meldungen

 Die Vertrauenswürdigkeit des Trustcenters konnte nicht ermittelt werden.

Signaturen

Zertifikat	Zeitpunkt der Signatur	Status des Zertifikats zum Zeitpunkt der Signatur
Name	Heute	 VALID

[Prüfergebnis als PDF](#) [Governikus Resultat](#)

Unter dieser Übersicht befinden sich zwei Schaltflächen, mit denen das Ergebnis als Prüfprotokoll genauer dargelegt wird. Mit 'Prüfergebnis als PDF' können Sie dieses Protokoll für Ihre Unterlagen ausdrucken oder herunterladen. Die Schaltfläche 'Governikus Resultat' führt Sie zu einer Browserversion des Protokolls.

4 Prüfprotokoll

Das Prüfprotokoll bietet Ihnen detaillierte Informationen zu den geprüften Signaturen sowie den Ergebnissen einzelner Prüfungen. Nachfolgend soll ein Überblick über den Inhalt des Prüfprotokolls gegeben werden.

- **Struktur:** Enthält grundsätzlich die oben beschriebenen Informationen Gesamtprüfergebnis, zur Prüfung herangezogene Dateien, sowie eine Auflistung der Autoren (Unterzeichner). Zusätzlich wird zu jedem Autor das zusammengefasste Ergebnis der Zertifikatsprüfung angezeigt. Durch einen Mausklick auf den Autorennamen werden Sie zu dem detaillierten Prüfergebnis innerhalb des Protokolls geführt.
- **Signaturprüfungen:** Dieser Abschnitt zeigt Detailergebnisse zu den einzelnen Signatur-Prüfungen an:
 - Signaturformat
 - Auszug aus dem Inhalt des Zertifikats, Signaturniveau und Signaturzeitpunkt. Durch einen Mausklick auf den Namen des Autors gelangen Sie zu der Detailansicht des jeweiligen Zertifikats
 - Das Ergebnis der Integritätsprüfung.
 - Das Ergebnis der Identitätsprüfung des Autors.
 - Tauglichkeit der Hash- und Chiffrieralgorithmen der Inhaltsdaten- und Zertifikatssignatur zum Zeitpunkt der Signaturerstellung sowie zum Zeitpunkt der Prüfung.
- **Detailansicht der Zertifikate:** Hier werden Ihnen die detaillierten Inhalte aller Zertifikate angezeigt.
- **Technische Informationen:** Diese Abschnitt enthält technische Informationen zur Prüfung des Zertifikats zum Prüfzeitpunkt.
- **Auszug aus dem Algorithmenkatalog:** Die Tauglichkeit der in den Signaturen verwendeten Algorithmen wird anhand eines Algorithmenkatalogs geprüft, der durch die Bundesnetzagentur veröffentlicht wird. An dieser Stelle werden Ihnen die verwendeten Algorithmen mit dem derzeitigen Gültigkeitsende dargestellt, unterschieden nach Verwendungszweck. Der Algorithmenkatalog wird nur angezeigt, wenn eine qualifizierte Signatur geprüft wurde.
- **Übertragungsinformationen:** Dieser Abschnitt wird nur angezeigt, wenn die Anfrage an das OCSP/CRL-Relay entweder nicht vertrauenswürdig erfolgen konnte oder das OCSP/CRL-Relay nicht erreichbar war.

5 Grundlagen

5.1 Elektronische Signatur

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

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

Authentizität und Integrität

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

Wie entsteht eine qualifizierte elektronische Signatur?

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

1. Berechnung des Hashwerts

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

0D9C3ECD FBE036E1750DE82A7863F1E6B6AC336B

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. Es besteht aus einem privaten (geheimen) und einem öffentlichen Schlüssel. Der private Schlüssel ist nur auf der Signaturkarte enthalten und kann von dort nicht entfernt werden. Der

öffentliche Schlüssel kann jedem zugänglich gemacht werden. Mit dem privaten Schlüssel wird der Hashwert verschlüsselt. Dazu wird vom Programm, also vom Governikus Signer, der Hashwert der Datei errechnet. Dieser wird dann an die Signaturkarte übergeben. Innerhalb der Signaturkarte wird dieser Hashwert verschlüsselt und danach wird der verschlüsselte Hashwert an das Programm zurückgegeben. Um den Missbrauch einer Signaturkarte zu verhindern, wird vor dem Verschlüsseln mit dem privaten Schlüssel die persönliche Identifikationsnummer (PIN) abgefragt. Erst bei korrekter PIN-Eingabe wird verschlüsselt.

3. Hinzufügen des Zertifikats

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

5.2 Signierte Datei

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

5.3 Verifizierung

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

5.4 Zertifikatsprüfung

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