



## Bedienungsanleitung für die

## fideAS<sup>®</sup> sign

### Onlineverifizierung von qualifiziert signierten PDF-Dateien.

Sie haben ein signiertes PDF bekommen und möchten nun die Signatur verifizieren, um sicher zu sein, dass der Absender wirklich der Absender ist und dass das Dokument seit dem Signieren nicht mehr verändert wurde?

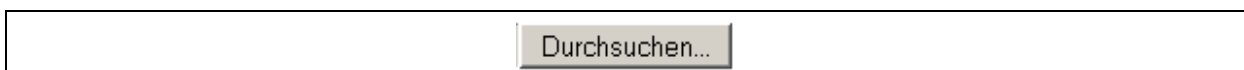
Die fideAS<sup>®</sup> sign Onlineverifizierung stellt die Richtigkeit von Signaturen sicher und gibt Ihnen ein entsprechendes Verifizierungsprotokoll zurück.

Die Onlineverifizierung ist leicht und ohne großen Aufwand bedienbar. Im Folgenden finden Sie eine Bedienungsanleitung und eine genaue Beschreibung der Protokollausgaben des Verifizierungsberichtes.

## 1 Die Startseite

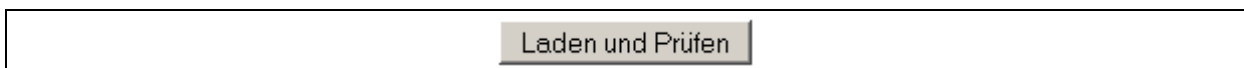
Über Ihren Webbrowser und die URL <https://www.apsec.de/sign> gelangen Sie zur Onlineverifizierung.

Über den Button „Durchsuchen“ können Sie eine PDF-Datei, die lokal auf Ihrem Computer gespeichert ist und deren Signatur verifiziert werden soll, auswählen.



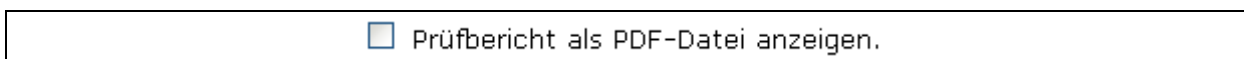
**Abbildung 1: Button „Durchsuchen...“ auf der Startseite**

Mit dem Button „Laden und Prüfen“ wird die Datei hochgeladen und im Hintergrund geprüft. Auf der nächsten Seite erscheint der passende Prüfbericht.



**Abbildung 2: Button „Laden und Prüfen“ auf der Startseite**

Mit dem Kontrollkästchen „Prüfbericht als PDF anzeigen“ wird festgelegt, ob der Prüfbericht als PDF-Datei angezeigt werden soll. Wird der Haken nicht gesetzt, wird der Prüfbericht als HTML-Seite angezeigt.



**Abbildung 3: Kontrollkästchen „Prüfbericht als PDF anzeigen“ auf der Startseite**



## Verifizierung von qualifiziert signierten PDF-Dokumenten

fideAS sign

Hier können Sie Ihr qualifiziert signiertes PDF-Dokument verifizieren. Wählen Sie dazu im Fenster "Durchsuchen" die PDF-Datei aus, die Sie überprüfen wollen und drücken Sie den "Laden und Prüfen"-Button. Das PDF wird hochgeladen und von unserer Software geprüft. Auf Ihrem Monitor erscheint der Report mit den Verifizierungsergebnissen.

Folgende Daten werden geprüft:

- ◆ **Integrität**  
Wurde das Dokument seit dem Signieren verändert?
- ◆ **Authentizität**  
Zeitliche Gültigkeit des Zertifikates  
Integrität des Zertifikates  
Prüfung gegen die Zertifikate des Ausstellers

Prüfungen gegen Sperrlisten, LDAP oder OCSP finden zur Zeit nicht statt.

Pfad für Dokument :

Durchsuchen...

**Hinweis:** Die Verbindung wird bei Dateien größer als 600kB abgebrochen.

Prüfbericht als PDF-Datei anzeigen.

Laden und Prüfen

[Nutzungsbedingungen](#) [Bedienungsanleitung](#)

Erstellen Sie noch keine e-Rechnungen, weil Ihnen noch vieles unklar ist? Zum Beispiel: Was sagt das Gesetz zur elektronischen Unterschrift? Ist es sehr aufwändig, die qualifizierte elektronische Signatur in meinem Unternehmen einzuführen? Wie schnell macht sich die Investition bezahlt? Fragen Sie uns! apsec berät Sie unverbindlich und ohne Fachchinesisch. Gleich ob Sie 100 oder 10.000 Rechnungen versenden - keine "pay per use" Kosten! Sie sparen Arbeitszeit, Papier-, Druckkosten, Portokosten und Platz, da die Papierarchivierung entfällt. Mehr Infos zu fideAS? sign hier: [www.apsec.de/m3-15.html](http://www.apsec.de/m3-15.html)

**Be sure. Be apsec.**

Abbildung 4: Startseite

## 2 Welche Dateien können geprüft werden?

Es werden alle PDF-Dateien geprüft, die folgende Voraussetzungen erfüllen:

- Die PDF-Version muss zwischen 1.3 und 1.5 sein.
- Nur nach PKKMS eingebettete Signaturen können geprüft werden.
- Das Zertifikat des Unterzeichners muss von einem Trustcenter ausgestellt sein, dessen Zertifikat die Applied Security GmbH zur Prüfung bereit stellt.
- Die Datei darf nicht größer als 600 KB sein.

### 3 Was wird geprüft ?

Geprüft werden die im PDF-Dokument eingebetteten Signaturen hinsichtlich:

- Integrität:
  - Wurde das Dokument seit dem Signieren verändert?
  - Falls es verändert wurde, wird geprüft, ob die unterschriebene Version des Dokumentes noch angezeigt werden kann oder, ob an dieser Änderungen vorgenommen wurden.
- Authentizität:
  - Ist das Zertifikat in Ordnung?
  - Wie ist die Gültigkeit des Zertifikates?
  - Wurde das Zertifikat von einem der von apsec vorgehaltenen Ausstellerzertifikate erzeugt und unterschrieben?

### 4 Welche Informationen liefert der Verifizierungsreport?

Der Verifizierungsreport liefert Informationen zu den Signaturen, die im Dokument eingebettet sind, und die Details für jede einzelne Signatur.

Im ersten Abschnitt des Verifizierungsreports finden Sie die Kopfzeile mit folgenden Informationen:

- Welche Signatur/en wurde/n verifiziert?
- Wie viele Signaturen enthält das Dokument?



**Abbildung 5: Kopfzeile des Verifizierungsreports (PDF-Dokument)**

Im zweiten Abschnitt des Verifizierungsreports finden Sie die Zertifikats- und Signaturinformationen (getrennt und für jede Signatur einzeln aufgeführt). Zunächst werden folgende Informationen angezeigt:

Signierender: Ersteller der Signatur.

Aussteller des Zertifikates: Trustcenter, das das zur Signatur verwendete Zertifikat ausgestellt hat.

Zeitpunkt der Signatur: Der Signatur mitgegebene Zeitangabe.

Ort der Signatur: Falls dieser bei der Signaturerstellung angegeben wurde.

Grund der Signatur: Falls dieser bei der Signaturerstellung angegeben wurde.




Signierender	C=DE; 0.2.262.1.10.7.20=1; CN=apsec SigG :PN
Aussteller des Zertifikats	C=DE; O=Deutsche Telekom AG; OU=Produktzentrum TeleSec; 0.2.262.1.10.7.20=1; CN=TeleSec PKS SigG CA 13:PN
Zeitpunkt der Signatur	20.09.2005 07:45:16
Ort der Signatur	Stockstadt
Grund der Signatur	Rechnungssignatur

**Abbildung 6: Zertifikats- und Signaturinformationen**

Unterhalb der Zertifikats- und Signaturinformationen wird die jeweilige Zusammenfassung und Schlussfolgerung der Verifizierung angezeigt.

Der Idealfall ist gegeben, wenn alle Kriterien (Überprüfung der Signatur und des Zertifikates) erfüllt sind. Dies bedeutet für Sie: Das Dokument wurde seit der Signaturerstellung nicht mehr verändert und der Ersteller der Signatur ist vertrauenswürdig. Die folgende Abbildung zeigt den Auszug eines solchen Prüfprotokolls.


**Signaturprüfung**

-  Das Dokument wurde nach dem Signieren nicht mehr verändert.
-  Die Zertifikatsprüfung war erfolgreich.  
Das Zertifikat ist gültig von **18.05.2005 13:25:05** bis **18.05.2007 13:25:05**
-  Das Zertifikat konnte erfolgreich gegen das Ausstellerzertifikat geprüft werden.

**Abbildung 7: erfolgreiche Verifizierung**

Können die Kriterien nicht vollständig - wie im Idealfall oben beschrieben - sichergestellt werden, werden die entsprechenden Meldungen mit einem blauen „i“ oder einem roten Kreuz gekennzeichnet. Diese Meldungen machen Sie darauf aufmerksam, dass eines oder mehrere der Kriterien, die unter Kapitel 2 und 3 aufgeführt sind, nicht erfüllt wurden.

**Meldung 1:**

 Das Dokument wurde nach der Signatur verändert. Die Integrität und Authentizität des Dokuments kann nur durch weitere Signaturen sichergestellt sein.

Hier liegt eine Veränderung des Dokuments nach der Erstellung der Signatur vor. Die Integrität des Dokuments ist nicht gegeben. Bitte fragen Sie beim Ersteller der Signatur nach dem unverfälschten Originaldokument mit entsprechender Signatur und prüfen Sie das neu erhaltene Dokument erneut.

### Meldung 2:



Das Dokument wurde nach dem Signieren verändert. (Dies kann durch das Anfügen weiterer Signaturen geschehen.)



Die unterschriebene Version des Dokuments wurde nach dem Signieren nicht mehr geändert. Sie kann mit entsprechenden Viewern angezeigt werden.

Grundsätzlich können innerhalb eines PDF-Dokuments mehrere Versionen gepflegt und verwaltet werden. Jede Version kann einzeln signiert werden. Bitte beachten Sie, dass ein Dokument, das bereits eine signierte Versionen enthält, durch das Anbringen einer weiteren Signatur verändert wird. Eine Änderung der ersten Version findet durch eine weitere Signatur nicht statt. Einzelne Versionen können Sie sich jederzeit mit dem Adobe Reader anzeigen lassen.

### Meldung 3:



Diese PDF Version wird nicht unterstützt.

Bei dem von Ihnen geladenen Dokument handelt es sich nicht um ein PDF-Dokument, das den unter Kapitel 2 angegebenen Voraussetzungen entspricht. Eine Verifizierung der Signatur ist leider nicht möglich.

### Meldung 4:



Das von Ihnen gesendete Dokument konnte nicht als PDF erkannt werden. Möglicherweise enthält der Dateiname ungültige Zeichen.

Bei allen Dokumenten, die nicht als PDF erkannt werden, erhalten Sie diese Meldung. Stellen Sie sicher, dass es sich bei der hochgeladenen Datei um ein PDF-Dokument handelt und verifizieren Sie es erneut.

### Meldung 5:



Es wurden keine Datei empfangen. Möglicherweise haben Sie versucht eine Datei grösser als 600kb hochzuladen.

Die Datei, die Sie hochzuladen versuchten, entspricht nicht der vorgegebenen Größe. Mit der Online-Verifizierung können nur Signaturen von Dateien bis 600kb verifiziert werden.

### Meldung 6:

Signierender	Konnte nicht ermittelt werden
Aussteller des Zertifikats	Konnte nicht ermittelt werden
Zeitpunkt der Signatur	20.12.2005 10:37:37
Ort der Signatur	
Grund der Signatur	

#### Signaturprüfung



Die Signatur enthält ein ungültiges Format und konnte nicht geprüft werden.

Die Signatur selbst wurde manipuliert und kann daher nicht geprüft werden. Bitte fragen Sie beim Ersteller der Signatur nach dem unverfälschten Originaldokument mit entsprechender Signatur und prüfen Sie das neu erhaltene Dokument erneut.

### Meldung 7:



Das PDF Dokument ist nicht signiert.

Das von Ihnen geladene Dokument enthält keine Signatur nach dem PKKMS-Standard.

### Meldung 8:



Die Signatur ist entweder nicht qualifiziert oder der Herausgeber des Zertifikats ist uns nicht bekannt.

Die Zertifikate der qualifizierten Trustcenter werden von Applied Security GmbH eingelesen und können anschließend zur Verifizierung verwendet werden. Ist das Zertifikat des Herausgebers nicht bekannt, kann das Zertifikat der Signatur nicht gegen ein Ausstellerzertifikat geprüft werden.