

**secunet**

*multisign*

# Signatur-Prüfwerkzeug Handbuch

**secunet** Security Networks AG

**secunet**

Stand: 24.06.05



## 1 Einleitung

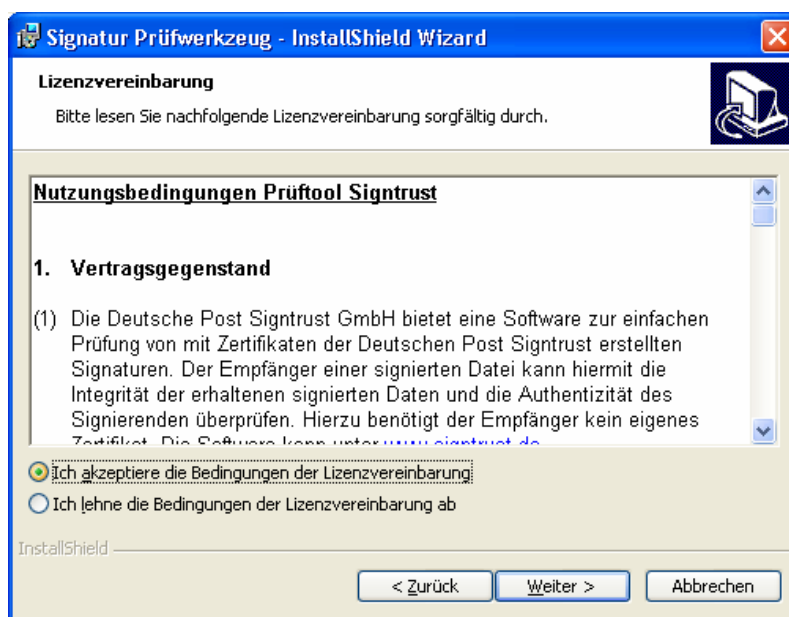
Die *multisign*-Produktfamilie ermöglicht die automatische Erstellung qualifizierter Signaturen. Eine Signatur ermöglicht einen zweifelfreien Nachweis über Herkunft und Integrität eines bestimmten Dokuments.

Mit Hilfe des *multisign* Signatur-Prüfwerkzeugs kann zu einem beliebigen Zeitpunkt überprüft werden, ob das Dokument tatsächlich von einem bestimmten Herausgeber stammt und ob es noch unverändert vorliegt.

## 2 Installation

Die Installation erfolgt unter den Betriebssystemen Microsoft Windows 2000/XP durch einen Doppelklick auf die Datei „*multisign Signatur Prüfwerkzeug.msi*“. Dadurch wird der InstallShield Wizard des Betriebssystems gestartet und Sie werden durch die Installation geführt.

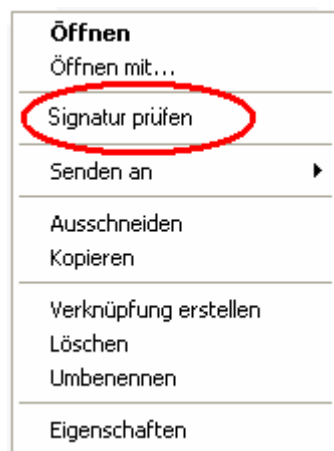
Zunächst werden Ihnen die Lizenzbedingungen des Prüfwerkzeugs angezeigt, die Sie zur Fortführung des Prozesses akzeptieren müssen.



Nach der Eingabe aller notwendigen Informationen wird das Prüfwerkzeug auf dem System installiert.

### 3 Benutzung

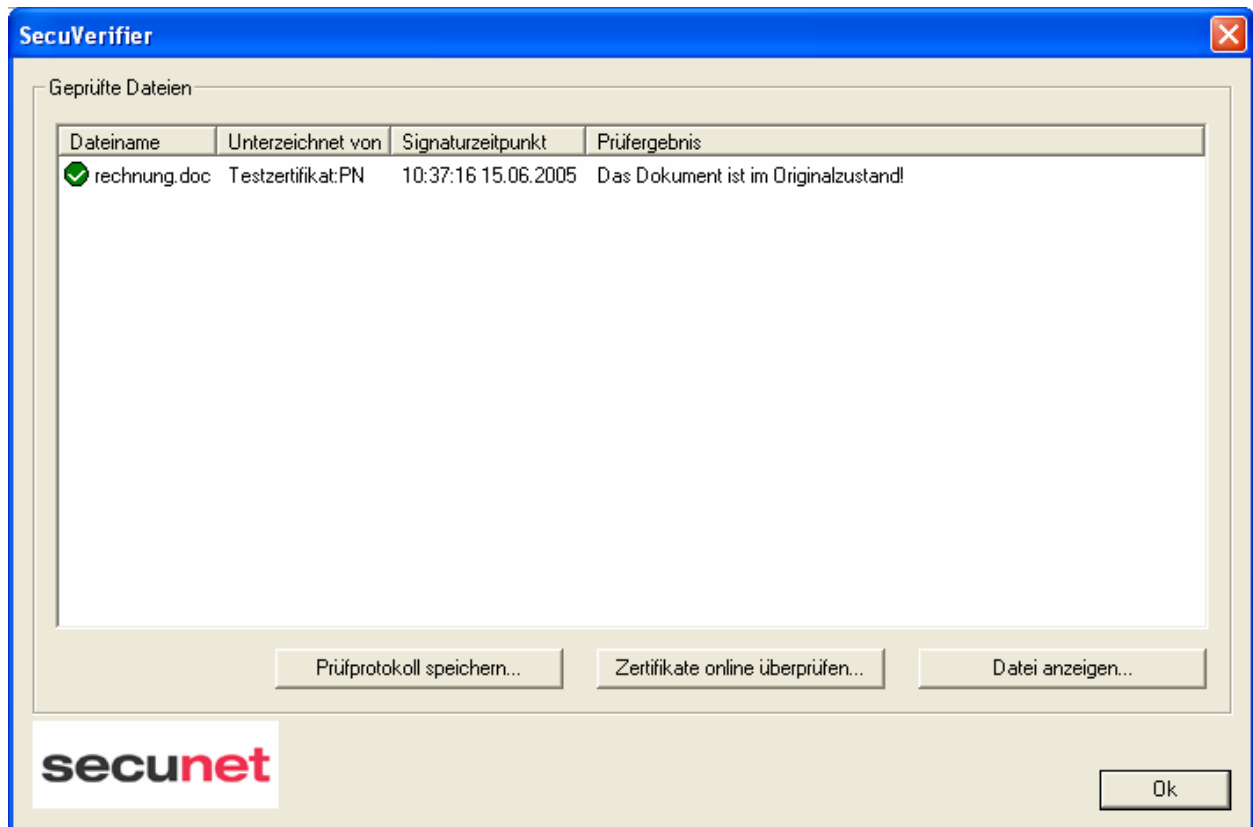
Im Gegensatz zu vielen anderen Anwendungen für das Prüfwerkzeug nicht vom Start-Menü aus gestartet. Es erweitert vielmehr das Kontextmenü (rechte Maustaste) des Windows Explorers um einen zusätzlichen Befehl „Signatur prüfen“



Dieser Befehl steht Ihnen immer zur Verfügung, wenn Sie eine oder mehrere Dateien vom Typ „PKCS#7“-Signatur (\*.p7s) ausgewählt haben. Sie können auch die Funktion „Signatur prüfen“ auch auf beliebige Ordner im Dateisystem anwenden, in diesem Fall werden alle Signaturdateien innerhalb dieses Ordners geprüft.

Zur Signaturprüfung muss neben der Signaturdatei auch das zugehörige Originaldokument vorhanden sein. Das Originaldokument muss den gleichen Namen wie die Signaturdatei haben, jedoch ohne die Dateiendung „.p7s“.

Nach der Prüfung aller Signaturen, werden die Ergebnisse in einem Dialog angezeigt.



Neben dem Dokumentnamen wird jeweils der Herausgeber der Signatur angezeigt. Durch einen Doppelklick auf eine Zeile können zusätzliche Informationen zu diesem Herausgeber dargestellt werden. In der dritten Spalte des Dialoges befindet sich das Prüfergebnis. Beim Prüfergebnis werden drei verschiedene Möglichkeiten unterschieden.

- Das Dokument befindet sich im Originalzustand.
- Das Dokument wurde manipuliert.
- Die Signatur des Dokuments konnte nicht geprüft werden.

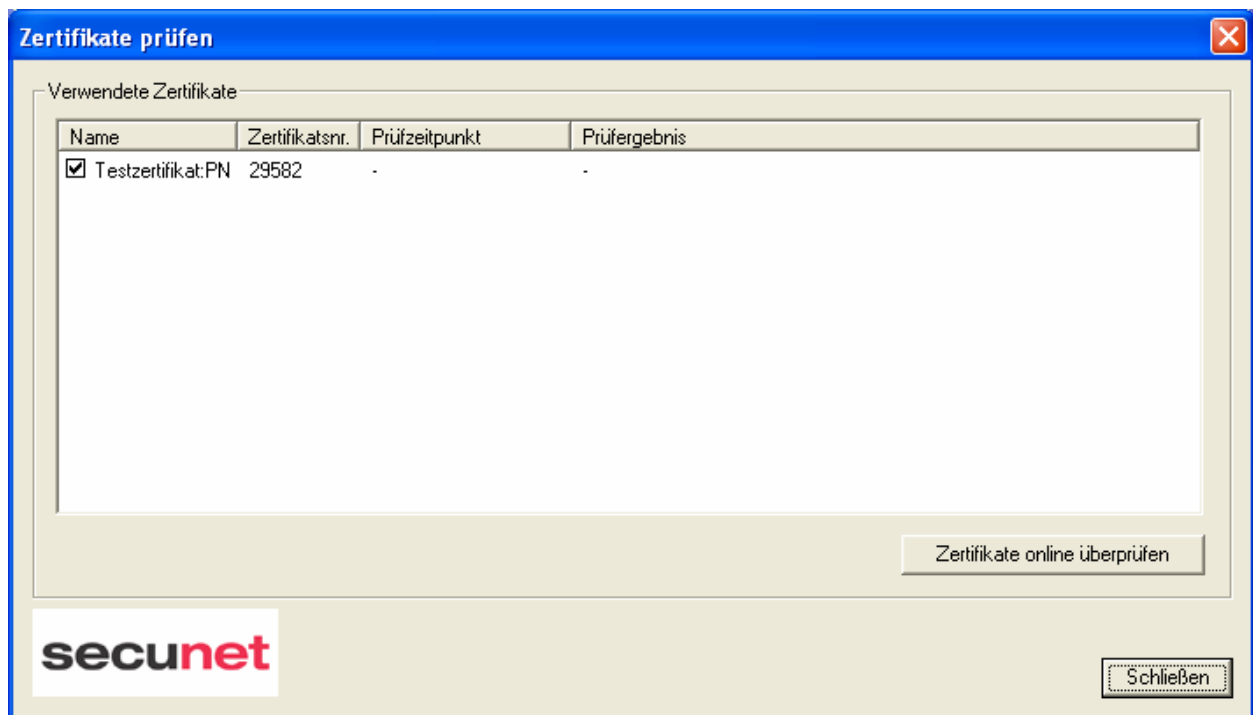
Wenn die Signatur des Dokuments nicht geprüft werden konnte, so kann keine Aussage darüber getroffen werden, ob das Dokument noch im Originalzustand ist. Die Ursache hierfür ist möglicherweise, dass die Signatur nicht den Anforderungen des Standards ISIS-MTT entspricht.

Der Inhalt der geprüften Originaldokumente kann durch Anklicken des Knopfes „Datei anzeigen“ dargestellt werden. Das aktuell ausgewählte Dokument wird innerhalb der Applikation geöffnet, die dem entsprechenden Dateityp zugeordnet wurde.

### 3.1 Online-Abfrage des Zertifikatsstatus

Zur Beurteilung der Gültigkeit einer Signatur ist neben der Unversehrtheit der Daten auch die Gültigkeit des verwendeten Zertifikats wichtig. Es muss festgestellt werden, ob das Zertifikat in der Zwischenzeit gesperrt wurde. Hierzu kann der Sperrstatus über eine Online-Anfrage beim jeweiligen Verzeichnisdienst ermittelt werden.

Nach dem Anklicken des Knopfes „Zertifikats online überprüfen“ werden in einem separaten Dialog alle Zertifikate angezeigt, die zur Signatur der geprüften Dokumente verwendet wurden. Wenn ein Zertifikat für mehrere Dokumente genutzt wurde, so erscheint es in diesem Dialog nur ein einziges Mal.



Innerhalb des Dialogs können die einzelnen Zertifikate an- und abgewählt werden. Durch Anklicken des Knopfes „Sperrstatus online abfragen“ wird für alle angewählten Zertifikate eine

Online-Anfrage beim Verzeichnisdienst gestellt. Dieses dauert je nach Anzahl der Zertifikate und der Verbindungsgeschwindigkeit mehrere Sekunden oder einige Minuten.

Die einzelnen Prüfergebnisse der Sperrstatusabfrage werden anschließend in dem Dialog angezeigt. Dem Ergebnis kann entnommen werden, ob und wenn ja seit wann ein Zertifikat gesperrt ist. Signaturen, die nach einer Sperrung des Zertifikats erstellt wurden, sind ungültig.

## 3.2 Prüfprotokoll speichern

Über den Knopf „Prüfprotokoll speichern“ kann das Prüfergebnis in eine Protokolldatei ausgegeben werden. Bei Betätigung dieser Schaltfläche wird der Benutzer nach einem Speicherort für die Protokolldaten gefragt, anschließend wird dort für jedes Prüfergebnis eine Protokolldatei angelegt, in der die Ergebnisdetails dokumentiert werden.

Es werden sowohl die Ergebnisse der Signaturprüfung, als auch ggf. der Sperrstatus der Signaturzertifikate protokolliert.

Der Name der Protokolldatei ergibt sich jeweils aus dem Namen der Originaldatei durch anhängen der Endung „.txt“. Existiert bereits eine solche Datei, so wird diese nach Rückfrage überschrieben

## 3.3 Format der Protokolldatei

Die Protokolldatei stellt eine normale Textdatei dar, in der jeweils ein Prüfergebnis dokumentiert wird. Jede Zeile der Protokolldatei enthält eine Ergebnisinformation im allgemeinen Format:

```
<Bezeichner>: <Wert>
```

Der Prüfzeitpunkt wird z.B. wie folgt dokumentiert:

```
Prüfzeitpunkt : 06.07.2004 12:13:50
```

Ein Protokolleintrag, der das Ergebnis einer Signaturprüfung dokumentiert, besteht aus folgenden Informationen.

Bezeichner	Beschreibung
Prüfzeitpunkt	Zeitpunkt der Signaturprüfung (lokale Systemzeit)
Dateiname	Pfad und Name der geprüften Datei
Signiert von	CommonName, Zertifikatsnummer und Aussteller des Signaturzertifikats
Signaturzeit	Zeitpunkt der Signaturerstellung
Prüfergebnis	Detaillierte Dokumentation des Prüfergebnisses
Sperrstatus	Antwort des Verzeichnisdienstes bei der Zertifikatsprüfung

Im Falle einer vollständig korrekten Signatur sieht somit ein Protokolleintrag wie folgt aus:

```
Prüfzeitpunkt: 06.07.2004 13:23:57
Dateiname: c:\SignierteDateien\RechungNr1.pdf.p7s
Signiert von: Erika Mustermann (Zertifikat 4711/Signtrust)
Signaturzeit: 03.01.2003 12:11:41
Prüfergebnis: Die Signatur wurde erfolgreich geprüft.
Sperrstatus: Laut Auskunft des Verzeichnisdienstes vom 06.07.2004 13:23:55 ist das
Signaturzertifikat nicht gesperrt.
```

Tritt bei einer Signaturprüfung ein Fehler auf, so wird dieser detailliert dokumentiert. Hierbei werden die Ergebnisse der Teilprüfungen einzeln in der folgenden Reihenfolge in die Protokolldatei aufgenommen.

- Die Signaturprüfung war nicht möglich, da die Datei mit den Originaldaten nicht vorhanden war.
- Die Signatur ist mathematisch falsch.
- Ein Zertifikat in der Zertifikatskette ist fehlerhaft.
- Die Zertifikatskette konnte nicht geprüft werden, da in der Signaturdatei nicht alle benötigten Zertifikate vorhanden waren.
- Das Signaturzertifikat ist seit dem dd.mm.yy abgelaufen.

Bei der Sperrstatusabfrage sind ebenfalls mehrere Fehlermeldungen möglich:

- Das Zertifikat ist seit dem dd.mm.yy gesperrt.
- Das Zertifikat ist im Verzeichnisdienst nicht bekannt.
- Der Verzeichnisdienst nicht ist momentan nicht verfügbar.