Kurzanleitung digiSeal®reader

Kostenfreie Software für die Prüfung elektronisch signierter Dokumente.

Erstellt von:
secrypt GmbH

Support-Hotline:
(0,99 EURO pro Minute aus dem deutschen Festnetz)
0900 1 732797 oder
0900 1 SECRYPT

Revisionshistorie:

Datum	Version	Bemerkung(en)	Autor(en)
24.11.2006	0.8	Initialversion	enen
01.12.2006	0.9	Überarbeitet / Geprüft / Freigegeben	enen
04.12.2006	1.0	Überarbeitet / Geprüft / Freigegeben	enen
26.04.2007	1.1	Überarbeitet / Geprüft / Freigegeben	nisc
10.03.2009	1.2	Überarbeitet / Geprüft / Freigegeben	kale
05.06.2009	1.3	Überarbeitet	kale / tami

secrypt GmbH
Bessemerstraße 82
D-12103 Berlin

www.secrypt.de

Inhaltsverzeichnis:

1. Vorteile des digiSeal reader

Prüfung aller gängigen Signaturformate
PDF, PKCS#7, XML-DSIG, XML-XAdES, EDI (Ideal Message Schweiz), 2D-Barcode-Signatur

Vollständige Durchführung der Signaturprüfung

1.) Prüfung der Integrität des Dokumentes – Wurde das Dokument verändert?
2.) Prüfung des Signaturzertifikats inklusive Zertifikatspfades sowie Prüfung, ob die Signatur bzw. das Signaturzertifikat "qualifiziert" ist.
3.) Online-Prüfung der Signaturberechtigung des Versenders beim entsprechenden Trustcenter.

Erstellung einer GDPdU-konformen Prüfdokumentation
(GDPdU: Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen)
Die Prüfdokumentation wird im PDF- und XML-Format erstellt und ist z.B. relevant beim Empfang und der Archivierung elektronisch signierter Rechnungen gemäß Umsatzsteuergesetz.

Weitere GRATISFUNKTION:
Verschlüsseln und Entschlüsseln von elektronischen Dokumenten
Die Ver- und Entschlüsselung kann mit Passwort oder Zertifikat des Empfängers erfolgen.
Es wird der starke internationale Standard AES mit 128 Bit Schlüsssellänge verwendet.
Durch die Nutzung dieser Gratisfunktion wird verhindert, dass unbefugte Dritte Einblick in sensible Dokumente erhalten.

2. Was ist eine elektronische Signatur?

Die elektronische Signatur ist etwas völlig anderes als die handschriftliche Unterschrift. Die elektronische Signatur basiert auf starken Verschlüsselungs- bzw. Kryptographieverfahren. Vereinfacht gesagt, ist sie ein Kryptogramm, welches einer elektronischen Datei, z.B. einer elektronischen Rechnung, beigefügt wird, um die Authentizität, Integrität und Beweisfähigkeit dieser Datei sicherstellen zu können.

Das technische Verfahren elektronischer Signaturen basiert auf der Verwendung zweier unterschiedlicher elektronischer Schlüssel (Signaturschlüsselpaar): dem privaten und dem öffentlichen Schlüssel.
Mit dem privaten Schlüssel (Private Key) erzeugt der Versender die elektronische Signatur. Im Fall der sogenannten "qualifizierten" elektronischen Signatur ist der private Schlüssel auf einer Signaturkarte bzw. Smartcard gespeichert. Mit dem sogenannten öffentlichen Schlüssel (Public Key) kann der Empfänger die Signatur prüfen.

3. Welche Schritte sind vom Empfänger bei der Prüfung elektronisch signierter Dokumente durchzuführen?

Für die Verifikation elektronisch signierter Dokumente - auch von FAX-Dokumenten - steht die Prüfsoftware digiSeal reader, die in beliebiger Anzahl kostenfrei als Internet-Download (auf www.secrypt.de) bereitgestellt wird, zur Verfügung.

Mit dieser Signaturprüfsoftware können sämtliche standardkonformen Signaturen unabhängig vom Softwarehersteller und Trustcenter geprüft werden.

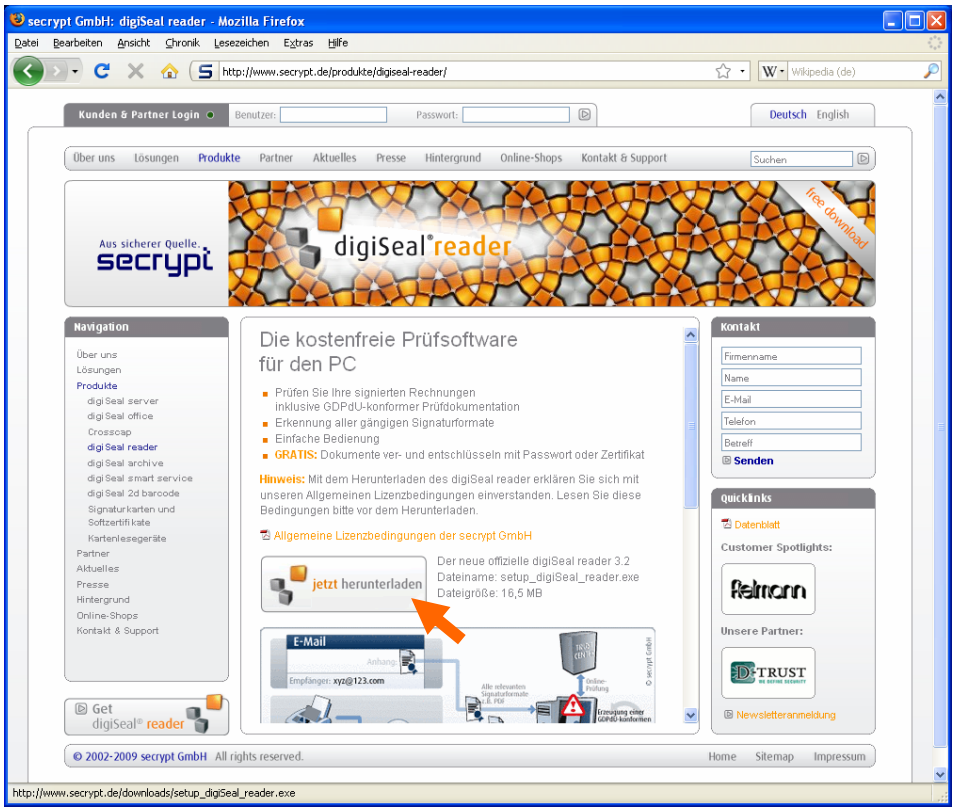
Im Fall einer elektronisch signierten Rechnung ist der Empfänger laut GDPdU (Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen) zur Prüfung der elektronischen Signatur und Dokumentation der Prüfung verpflichtet.

Mit der kostenfreien Prüfsoftware digiSeal reader wird dem Rechnungsempfänger die Möglichkeit gegeben, die empfangenen, qualifiziert signierten Rechnungen zu verifizieren, um damit den Verifikationsvoraussetzungen der entsprechenden Regelungen (GDPdU, BMF v. 29.01.2004, etc.) zu genügen.

3.1. Prüfschritte mit dem digiSeal reader

Schritt 1: Software-Download

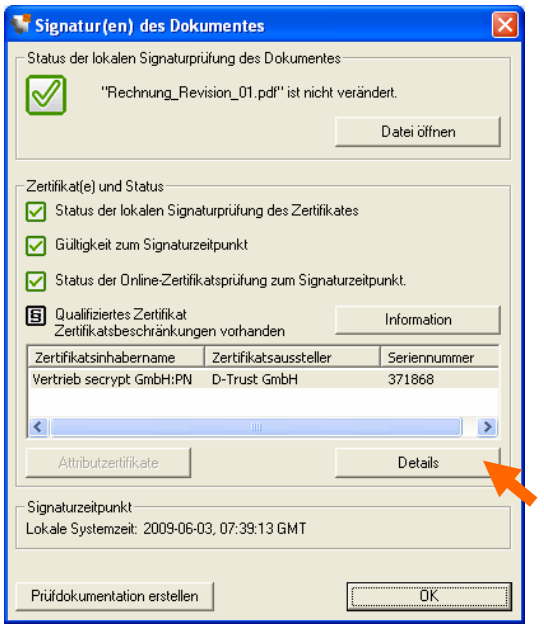
Download der kostenfreien Prüfsoftware digiSeal reader (auf www.secrypt.de) und Installation.



Schritt 2: Signiertes Dokument öffnen und prüfen

Öffnen Sie das Dokument (z.B. eine Rechnung) als Datei oder scannen Sie den Papierausdruck mit 2D-Barcode direkt über den digiSeal reader ein.

Die Signaturprüfung erfolgt anschließend automatisch und das Prüfergebnis wird in einem Fenster angezeigt. Über die Schaltfläche "Details" können Sie sich die Zertifikatsinhalte anzeigen lassen.



Bei der Signaturprüfung werden automatisch mehrere interne Schritte durchgeführt, u.a.:

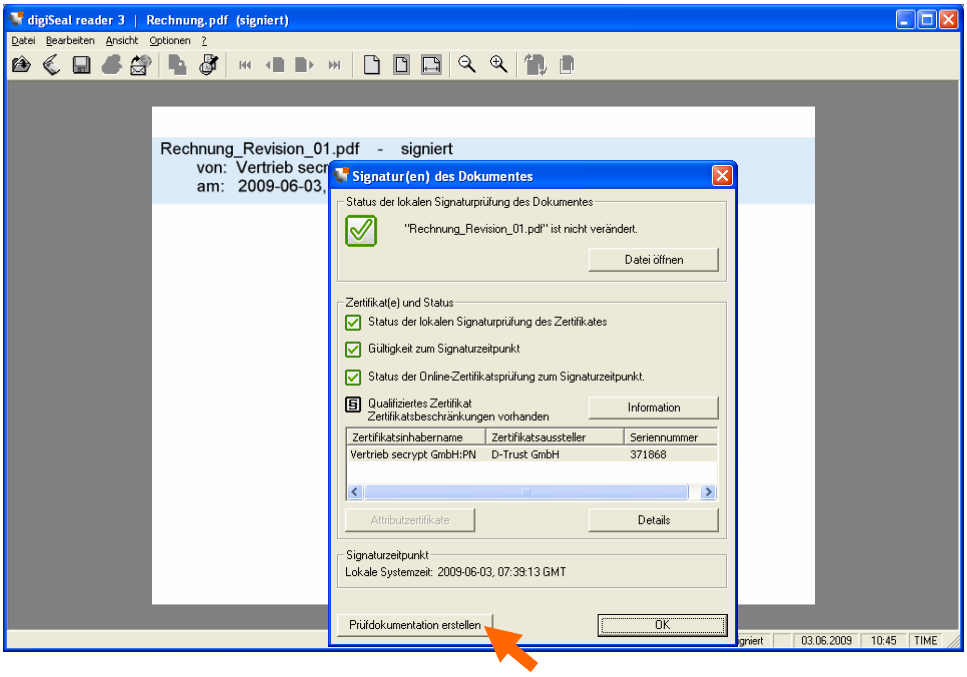
1.) Es wird geprüft, ob das Dokument verändert worden ist. Dazu ist keine Online-Verbindung notwendig.

2.) Es wird geprüft, ob die Signatur (bzw. das verwendete Signaturzertifikat) "qualifiziert" ist (Paragraphen-Symbol).

3.) Es wird die Signaturberechtigung des Versenders online bei dem betreffenden Trustcenter, welches dem Rechnungsversender die Signatur ausgestellt hat, geprüft.
Voraussetzung ist eine Internetverbindung. Falls die Internetverbindung über einen Proxyserver erfolgt, können unter dem Menüpunkt "Optionen / Einstellungen Online-Dienste" in den Feldern "Servername" und "Port" die entsprechenden Einträge vorgenommen werden.

Schritt 3: Prüfdokumentation erstellen (GDPdU-konform)

Durch Betätigen der Schaltfläche "Prüfdokumentation erstellen" wird automatisch sowohl eine PDF- als auch XML-Prüfdokumentation in einem von Ihnen zuvor definierten Ordner gespeichert.

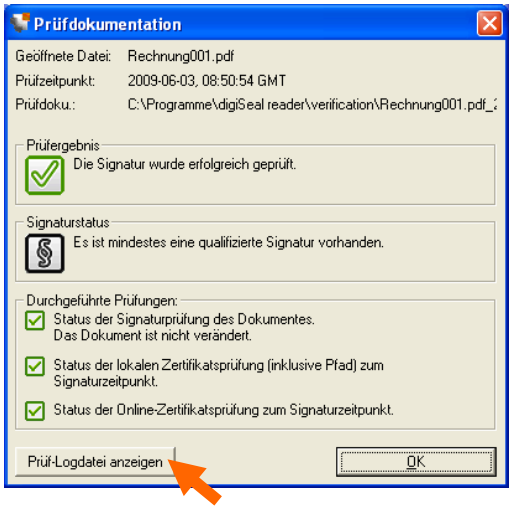


Dabei werden folgende Aktionen durchgeführt:

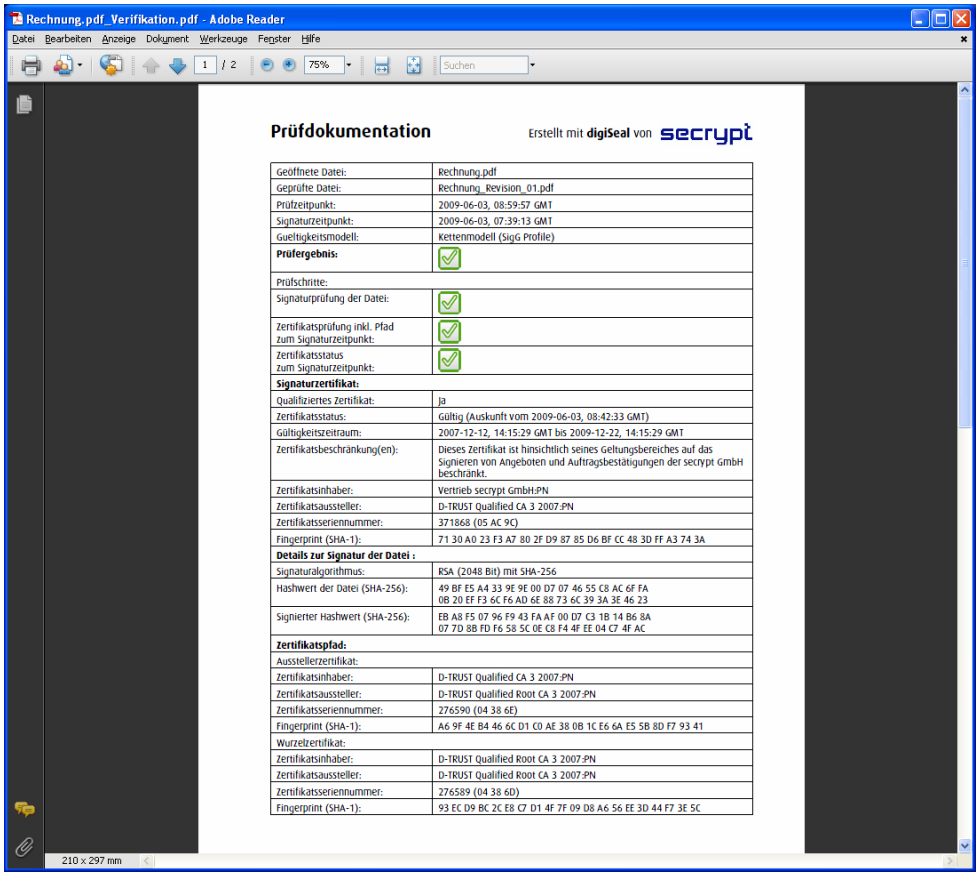
1.) Es wird eine XML-Prüf-Logdatei und eine PDF-Prüf-Logdatei erstellt, welche die Signaturprüfung detailliert dokumentieren.

2.) Es wird automatisch ein Ordner angelegt, in dem sämtliche Informationen, die eine Prüfdokumentation umfasst, gespeichert werden. Unter dem Menüpunkt "Optionen / Einstellungen allgemein" kann das gewünschte Verzeichnis zur Speicherung der Prüfdokumentation gewählt werden. Bei der elektronischen Archivierung z.B. einer Rechnung und der Prüfdokumentation ist dieser Ordner mit seinen Inhalten aufzubewahren.

3.) Die Ergebnisse werden in einem neuen Fenster "Prüfdokumentation" angezeigt.



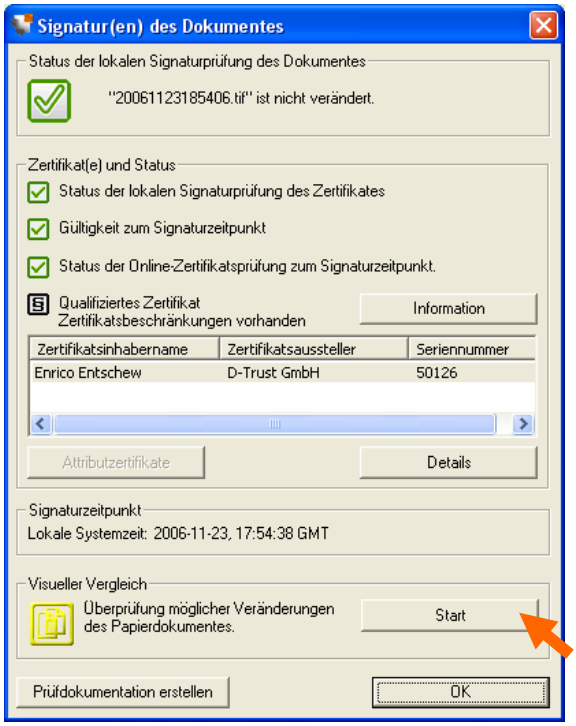
Durch Betätigung der Schaltfläche "Prüf-Logdatei anzeigen" wird die PDF-Prüfdokumentation angezeigt.



Geöffnete Datei:	Rechnung.pdf
Geprüfte Datei:	Rechnung_Revision_01.pdf
Prüfzeitpunkt:	2009-06-03, 08:59:57 GMT
Signaturzeitpunkt:	2009-06-03, 07:39:13 GMT
Gueltigkeitsmodell:	Kettenmodell (SigG Profile)
Prüfergebnis:	☑
Prüfschritte:	
Signaturprüfung der Datei:	☑
Zertifikatsprüfung inkl. Pfad zum Signaturzeitpunkt:	☑
Zertifikatsstatus zum Signaturzeitpunkt:	☑
Signaturzertifikat:	
Qualifiziertes Zertifikat:	Ja
Zertifikatsstatus:	Gültig (Auskunft vom 2009-06-03, 08:42:33 GMT)
Gültigkeitszeitraum:	2007-12-12, 14:15:29 GMT bis 2009-12-22, 14:15:29 GMT
Zertifikatsbeschränkung(en):	Dieses Zertifikat ist hinsichtlich seines Geltungsbereiches auf das Signieren von Angeboten und Auftragsbestätigungen der secrypt GmbH beschränkt.
Zertifikatsinhaber:	Vertrieb secrypt GmbH:PN
Zertifikatsaussteller:	D-TRUST Qualified CA 3 2007:PN
Zertifikatsseriennummer:	371868 (05 AC 9C)
Fingerprint (SHA-1):	71 30 A0 23 F3 A7 80 2F D9 87 85 D6 BF CC 48 3D FF A3 74 3A
Details zur Signatur der Datei :	
Signaturalgorithmus:	RSA (2048 Bit) mit SHA-256
Hashwert der Datei (SHA-256):	49 BF E5 A4 33 9E 9E 00 D7 07 46 55 C8 AC 6F FA 0B 20 EF F3 6C F6 AD 6E 88 73 6C 39 3A 3E 46 23
Signierter Hashwert (SHA-256):	EB A8 F5 07 96 F9 43 FA AF 00 D7 C3 1B 14 B6 8A 07 7D 8B FD F6 58 5C 0E C8 F4 4F EE 04 C7 4F AC
Zertifikatspfad:	
Ausstellerzertifikat:	
Zertifikatsinhaber:	D-TRUST Qualified CA 3 2007:PN
Zertifikatsaussteller:	D-TRUST Qualified Root CA 3 2007:PN
Zertifikatsseriennummer:	276590 (04 38 6E)
Fingerprint (SHA-1):	A6 9F 4E B4 46 6C D1 C0 AE 38 0B 1C E6 6A E5 5B 8D F7 93 41
Wurzelzertifikat:	
Zertifikatsinhaber:	D-TRUST Qualified Root CA 3 2007:PN
Zertifikatsaussteller:	D-TRUST Qualified Root CA 3 2007:PN
Zertifikatsseriennummer:	276589 (04 38 6D)
Fingerprint (SHA-1):	93 EC D9 BC 2C E8 C7 D1 4F 7F 09 D8 A6 56 EE 3D 44 F7 3E 5C

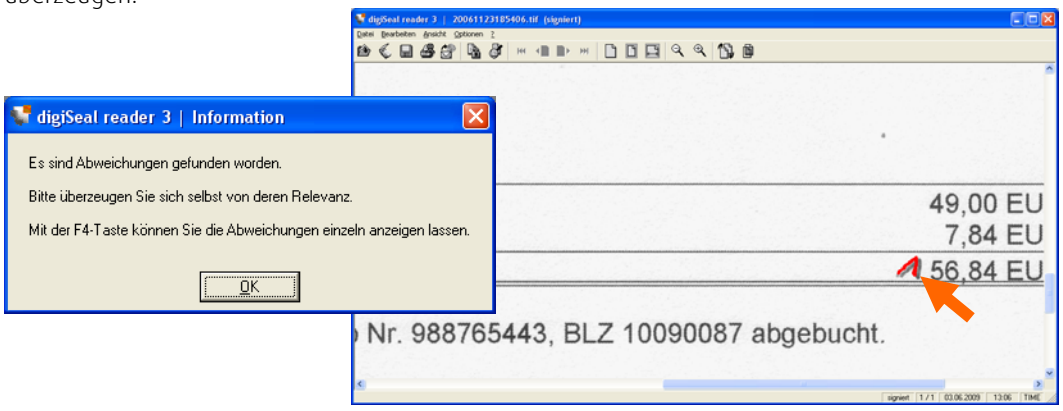
3.2. Besonderheiten bei 2D-Barcode-Dokumenten

Neben der automatischen Signaturprüfung des eingescannten Dokumentes können Sie den Papierinhalt von 2D-Barcode-Dokumenten zusätzlich auf Manipulationen prüfen (optional). Bitte betätigen Sie hierfür unter "Visueller Vergleich" die Schaltfläche "Start".



Anschließend wird der Vergleich des aus dem 2D-Barcode rekonstruierten mit dem eingescannten Dokument automatisch durchgeführt.

Das Ergebnis des visuellen Vergleichs wird angezeigt, wobei ggfs. vorhandene Abweichungen farblich markiert werden. Der Visuelle Vergleich ist ein unverbindliches Hilfsmittel. Der Betrachter hat sich in jedem Fall zusätzlich von der Relevanz der angezeigten Ergebnisse selbst zu überzeugen.



4. Weitere Funktionen des digiSeal reader

Der digiSeal reader unterstützt neben der Signaturverifikation aller gängigen Signaturformate auch das Ver- und Entschlüsseln von Dateien mit Passwort und mit Zertifikat sowie das Versenden von Dokumenten im Anhang einer E-Mail.

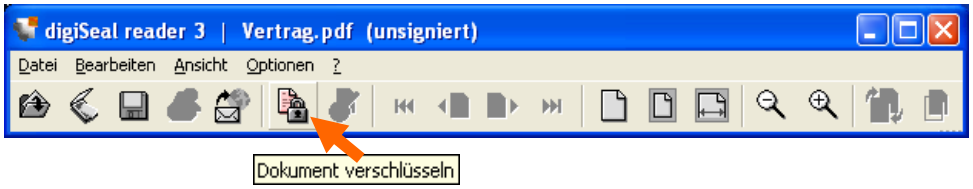
4.1. Ver- und Entschlüsselung von elektronischen Dokumenten

Als GRATISFUNKTION wird das Ver-und Entschlüsseln beliebiger Dateien mit Passwort (auf Basis des neuen internationalen Standards AES mit 128 Bit Schlüsssellänge) und mit Empfängerzertifikat angeboten. Damit wird sichergestellt, dass kein unbefugter Dritter Einblick in vertrauliche Daten erhält. Es können Dokumente beliebiger Dateiformate verschlüsselt werden, die im Anschluss im *.pk7- oder *.p7m-Format abgespeichert werden.

4.1.1. Verschlüsselung durchführen

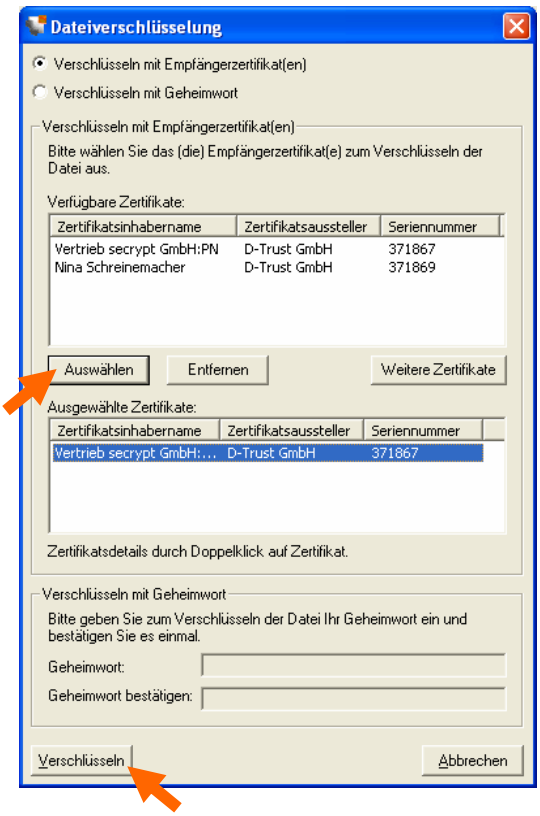
Schritt 1:

Betätigen Sie die Schaltfläche "Dokument verschlüsseln".



Schritt 2:

In dem sich öffnenden Fenster "Dateiverschlüsselung" kann das gewünschte Passwort oder Zertifikat (oder mehrere), mit dem die Datei verschlüsselt werden soll, ausgewählt werden ("Auswählen"-Schaltfläche).

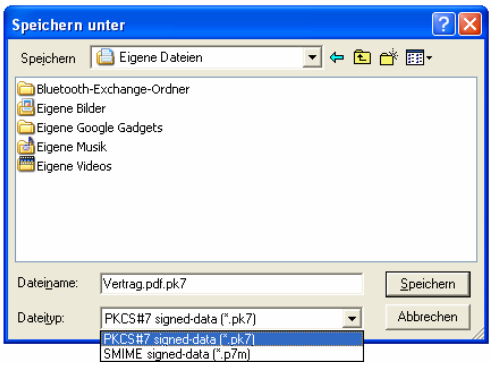


Schritt 3:

Zum Verschlüsseln der Datei mit dem zuvor ausgewählten Passwort oder Zertifikat ist die "Verschlüsseln"-Schaltfläche zu betätigen.

Schritt 4:

Die verschlüsselte Datei kann im *.pk7- oder *.p7m-Format an einem beliebigen Ort abgespeichert und dem Empfänger übermittelt werden.



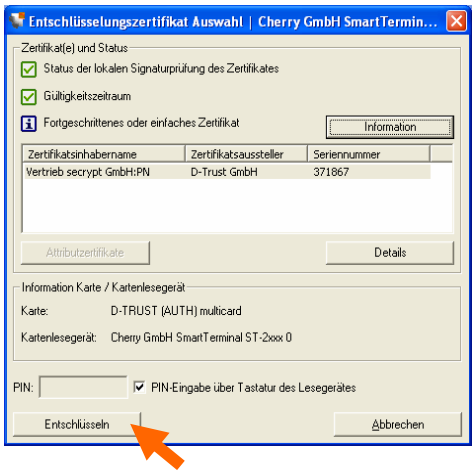
4.1.2. Entschlüsselung durchführen

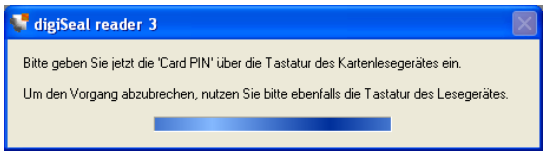
Schritt 1:

Die verschlüsselte *.pk7- oder *.p7m-Datei kann über die Schaltfläche "Öffnen und Prüfen" oder per "Drag&Drop" in digiSeal reader geladen werden.

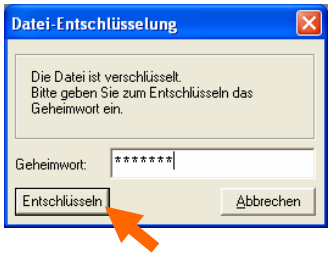
Schritt 2:

a) Mit Zertifikat entschlüsseln: Das karten- oder softwarebasierte Zertifikat ist auszuwählen. Falls sich das Zertifikat auf einer Chipkarte befindet, ist diese in das Kartenlesegerät einzuführen. Zum Entschlüsseln der Datei ist die PIN bzw. das Geheimwort einzugeben.





b) Mit Passwort entschlüsseln: Das entsprechende Passwort ist einzugeben und die "Entschlüsseln"-Schaltfläche ist zu betätigen.



Schritt 3:

Bei korrekter Eingabe wird die Datei entschlüsselt und angezeigt. Die entschlüsselte Datei kann anschließend im *.pk7- oder *.p7m-Format an einem beliebigen Ort abgespeichert werden.

4.2. E-Mail-Versand

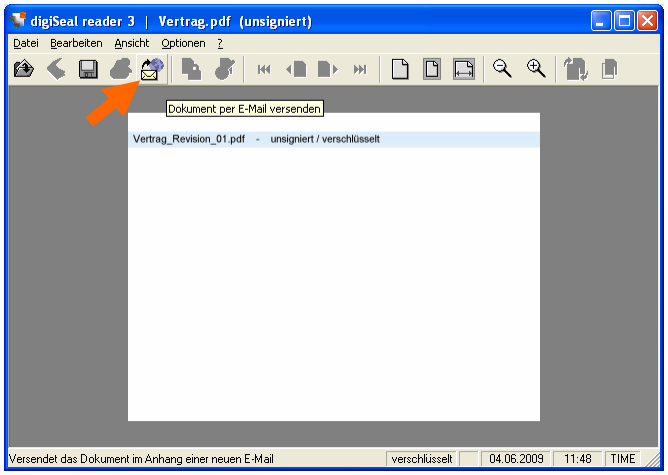
Ein im digiSeal reader geöffnetes (z.B. verschlüsseltes) Dokument kann direkt aus dem digiSeal reader heraus im Anhang einer E-Mail versendet werden.

Schritt 1:

Das zu versendende Dokument ist im digiSeal reader geöffnet. Bevor Sie es per E-Mail versenden können, muss es abgespeichert werden.

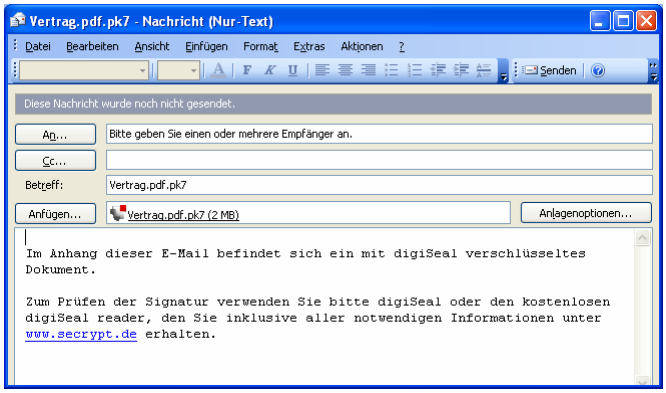
Schritt 2:

Betätigen Sie die Schaltfläche "Dokument per E-Mail versenden" oder gehen Sie über das Menü "Datei / Senden an...".



Schritt 3:

Es öffnet sich eine neue E-Mail in Ihrem als Standard eingestellten E-Mail-Client mit dem Dokument im Anhang.



Hinweis:

Achten Sie darauf, dass in Ihrem E-Mail-Client ein E-Mail-Konto ein-gerichtet ist, ansonsten ist der digiSeal reader nicht in der Lage, das Versenden durchzuführen.

Schritt 4:

Jetzt können Sie wie gewohnt Ihren Text in die E-Mail schreiben und die E-Mail versenden.