

Kurzanleitung digiSeal® reader

Seite 1 von 10

Die kostenfreie Software für die Prüfung
elektronisch signierter Dokumente



secrypt GmbH
Bessemerstraße 82
D-12103 Berlin

Stand: 30.06.2011

Support-Hotline:

(0,99 EURO pro Minute aus dem deutschen Festnetz)
0900 1 732797 oder
0900 1 SECRIPT

Revisionshistorie:

Datum	Dok.- 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
30.06.2011	2.0	Überarbeitet	frzi
29.08.2011	2.1	Überarbeitet	frzi

Inhaltsverzeichnis:

1.	Vorteile des digiSeal® reader.....	3
2.	Was ist eine elektronische Signatur?.....	3
3.	Welche Schritte sind vom Empfänger bei der Prüfung elektronisch signierter Dokumente durchzuführen?	4
3.1.	Prüfschritte mit dem digiSeal® reader.....	4
3.2.	Besonderheiten bei 2D-Barcode-Dokumenten	7
4.	Weitere Funktionen des digiSeal® reader	8
4.1.	Ver- und Entschlüsselung von elektronischen Dokumenten	8
4.1.1.	Verschlüsselung durchführen	8
4.1.2.	Entschlüsselung durchführen	9
4.2.	E-Mail-Versand.....	10

1. Vorteile des digiSeal® reader

Prüfung aller gängigen Signaturformate

PDF, PKCS#7, XML-DSIG, XML-XAdES, EDI, 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 Schlüssellänge 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, beigelegt 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

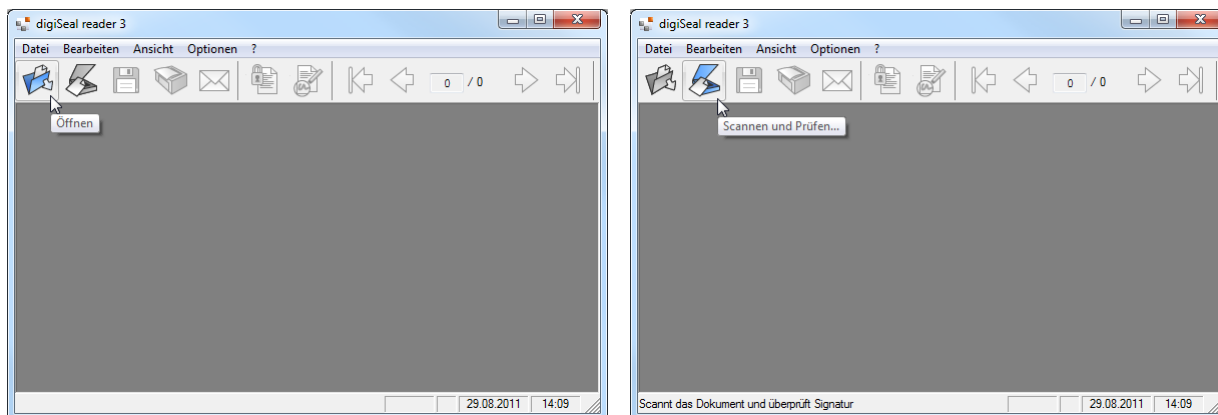
Schritt 1: Software-Download

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

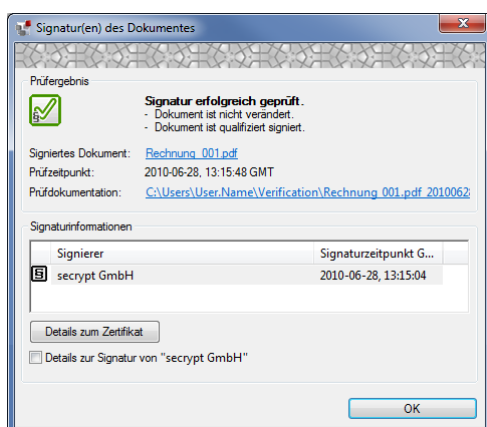
The screenshot shows the website <http://www.secrypt.de/produkte/digiseal-reader/>. The page layout includes a top navigation bar with links for 'Kontakt', 'Support', 'Downloads', 'Presse', and 'Shop'. A main navigation menu is visible with categories like 'Produkte', 'Wissen', 'Partner', and 'Über uns'. The 'Produkte' menu is expanded, showing a list of products including 'digiSeal® server', 'digiSeal® office', 'digiSeal® office pro', 'digiSeal® reader' (highlighted), 'digiSeal® archive', and 'digiSeal® 2d barcode'. A central banner features the text 'Ist die Unterschrift echt? Beliebige elektronisch signierte Dokumente gratis überprüfen'. Below this, the heading reads 'digiSeal reader – Die kostenfreie Software für die Signaturprüfung'. A 'Downloads & Quicklinks' section contains a 'Download digiSeal reader' button, which is highlighted with a red arrow. To the right of the button, technical specifications are listed: 'Offizielle Version 3.3', 'für Microsoft Windows® 7 / Vista / XP / 2000', 'Dateiname: setup_digiSeal_reader.exe', and 'Dateigröße: ca.11 MB'. At the bottom of the page, there is a small diagram illustrating the software's use and a text block stating: 'Dokumente, die mit einer elektronischen Signatur versehen sind, gewährleisten rechtskonforme Geschäftsprozesse in der digitalen Welt. Sie werden nach dem Signieren etwa per E-Mail verschickt. Der Empfänger des signierten elektronischen Dokuments kann dieses mit dem kostenlosen digiSeal® reader von secrypt auf einfache Weise prüfen – und damit dessen'.

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 zum Zertifikat" 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 (Paragrafen-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.

Kurzanleitung digiSeal® reader

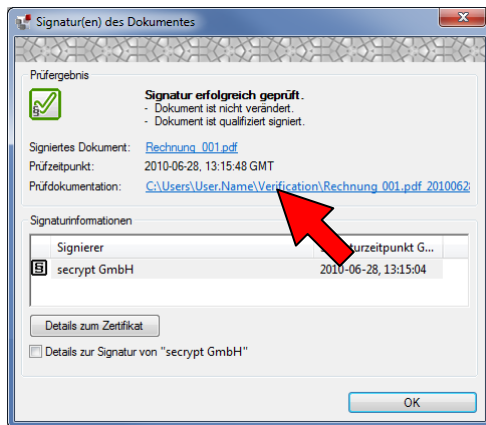
Schritt 3: Prüfdokumentation erstellen (GDPdU-konform)

Es wird automatisch sowohl eine PDF- als auch XML-Prüfdokumentation erstellt.

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.

Durch Klick auf den Link "Prüfdokumentation" wird die PDF-Prüfdokumentation angezeigt.

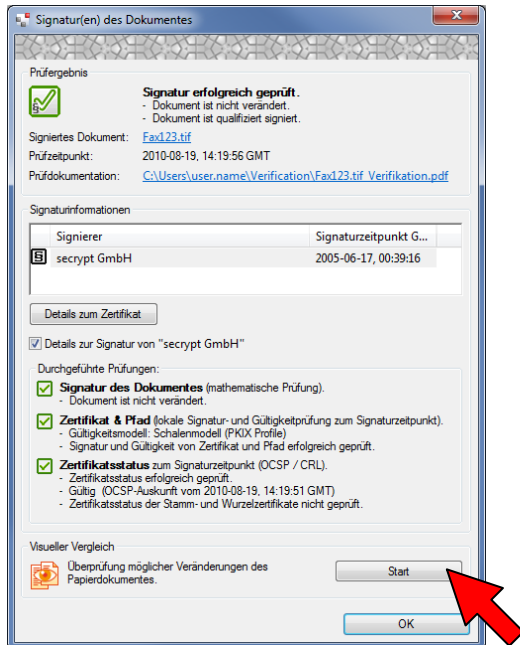


Prüfdokumentation		Erstellt mit digiSeal von secript
Geöffnete Datei:	Rechnung_001.pdf	
Geöffnete Datei:	Rechnung_001.pdf.pk7	
Prüfzeitpunkt:	2010-06-28, 13:15:48 GMT	
Signaturzeitpunkt:	2010-06-28, 13:15:04 GMT	
Geprüfte Daten:	Rechnung_001.pdf	
Prüfergebnis:	Die Signatur wurde erfolgreich geprüft.	
Prüfartefakte:		
Signaturprüfung der Daten:	[✓]	
Zertifikatsprüfung inkl. Pfad zum Signaturobjekt:	[✓]	
Zertifikatsstatus zum Signaturzeitpunkt:	[✓]	
Signaturzertifikat:		
Qualifiziertes Zertifikat:	ja	
Zertifikatsstatus:	Gültig (Ausw. vom 2010-06-28, 13:15:20 GMT)	
Gültigkeitsraum:	2008-07-19 09:02:45 GMT bis 2010-08-29, 09:02:45 GMT	
Zertifikatsinhaber:	secript GmbH/PA	
Zertifikatsaussteller:	D-TRUST Qualified CA 1 2008/PA	
Zertifikatsnummer:	52008 (00 EF 48)	
Fingerprint (SHA-1):	A9 91 55 5C 25 27 E1 83 68 9C K5 25 DK 88 41 47 A1 30	
Details zur Signatur der Datei:		
Signaturalgorithmus:	RSA (2048 Bit) mit SHA-256	
Hashwert der Datei (SHA-256):	34 B9 95 0A FE 4B 36 60 42 2C 00 96 67 68 DA E3 8E 0F 13 56 88 E6 03 3B 89 2A 94 3F E9 62 8D DA	
Signierter Hashwert (SHA-256):	73 04 92 44 64 BA 70 A3 48 85 20 A3 B1 78 88 8B 93 8B A6 44 42 12 82 79 64 8E 54 8C 18 64 99 2C	
Algorithmusstärke:	[✓] RSA (2048 Bit) geeignet bis einschließlich 2015-12-31. SHA-256 geeignet bis einschließlich 2015-12-31.	
Zertifikatspfad:		
Angewandtes Zertifikat:		
Zertifikatsinhaber:	D-TRUST Qualified CA 1 2008/PA	
Zertifikatsaussteller:	D-TRUST Qualified Root CA 1 2008/PA	
Zertifikatsnummer:	535121 (00 DK 31)	
Fingerprint (SHA-1):	91 23 FA F4 39 0D E5 92 90 41 A1 9E 17 57 7B E9 95 6A 90 E1	
Algorithmusstärke:	[✓] RSA (2048 Bit) geeignet bis einschließlich 2015-12-31. SHA-256 geeignet bis einschließlich 2015-12-31.	
Zertifikatsstatus:	Nicht geprüft	
Gültigkeitsraum:	2008-07-24, 16:54:11 GMT bis 2013-07-24, 15:30:00 GMT	
Wurzelschein:		
Zertifikatsinhaber:	D-TRUST Qualified Root CA 1 2008/PA	
Zertifikatsaussteller:	D-TRUST Qualified Root CA 1 2008/PA	
Zertifikatsnummer:	535120 (00 DK 30)	

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.

Beispiel für das unverbindliche Ergebnis eines Bildvergleichs

zeichnung	Höhe	Breite	Tiefe	MC	E-Preis	G-Preis
-Nr.: 94036010						
chenplatte	2,9	200,0				
chgehende Sockelplatte	5,4	180,0				
geschl., Aussenvergl.				423	386,00	386,00
Ahom Natur	115,2	40,0	37,0			
and 6 Raster				211	46,00	146,00

Rote Färbung: Inhalte, die nachträglich aus dem Papierdokument entfernt worden sind.

Blaue Färbung: Inhalte, die nachträglich in das Papierdokument eingefügt worden sind.

4. Weitere Funktionen des digiSeal® reader

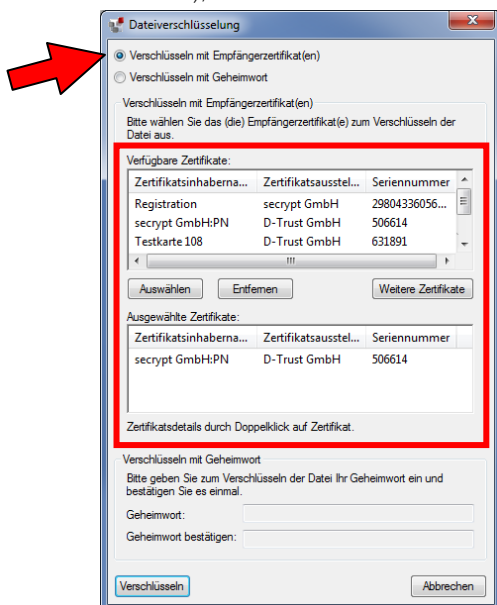
Der digiSeal® reader unterstützt neben der Signaturverifikation aller gängigen Signaturformate auch das Ver- und Entschlüsseln von Dateien mit Passwort und mit Zertifikat sowie das Versenden von Dokumenten im Anhang einer E-Mail.

4.1. Ver- und Entschlüsselung von elektronischen Dokumenten

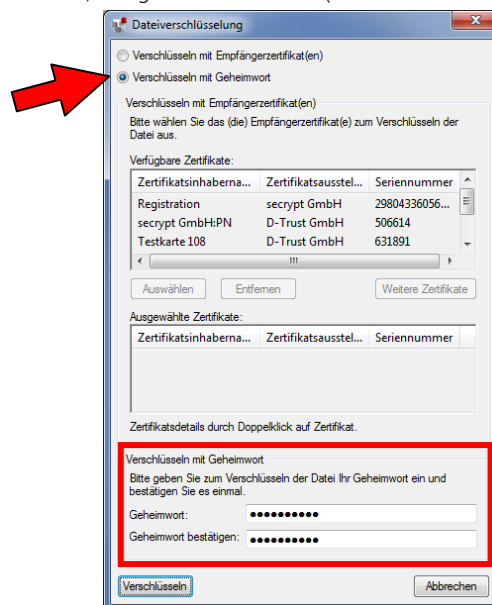
Als GRATISFUNKTION wird das Ver- und Entschlüsseln beliebiger Dateien mit Passwort (auf Basis des internationalen Standards AES mit 128 Bit Schlüssellänge) und mit Empfängerzertifikat angeboten. Damit wird sichergestellt, dass kein unbefugter Dritter Einblick in vertrauliche Daten erhält. Es können Dokumente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

4.1.1. Verschlüsselung durchführen

1. Wählen Sie aus der Kryptographie-Werkzeugleiste den Befehl "Dokument verschlüsseln"
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).



Verschlüsseln mit Zertifikat

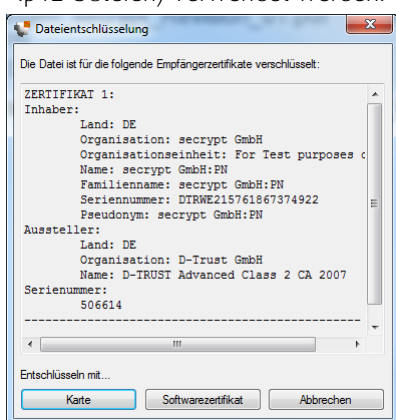


Verschlüsseln mit Geheimwort

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

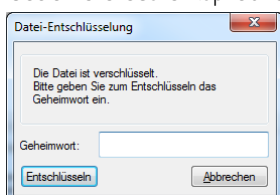
1. Die verschlüsselte *.pk7- oder *.p7m-Datei kann über die Schaltfläche "Öffnen und Prüfen" oder per "Drag&Drop" in digiSeal® reader geladen werden.
2. a) Mit Empfängerzertifikat(en)
Es wird automatisch nach geeigneten Zertifikaten gesucht. Sollte kein passendes Zertifikat für die Entschlüsselung zur Verfügung stehen, können Sie in einem nachfolgenden Schritt weitere Optionen wählen. Wählen Sie "Karte", wenn Sie ein Zertifikat von einer Smartcard nutzen wollen oder wählen Sie "Softwarezertifikat", wenn Sie ein Softwarezertifikat verwenden wollen. In diesem Fall werden Sie aufgefordert, den Speicherort des Zertifikats anzugeben. Hierfür können PKCS#12-Zertifikate (*.pfx- oder *.p12-Dateien) verwendet werden.



Zum Entschlüsseln werden Sie schließlich aufgefordert, Ihre Karten-PIN bzw. Ihr Geheimwort (Softwarezertifikat) einzugeben.

b) Mit Geheimwort

Geben Sie das entsprechende Geheimwort ein und die klicken Sie anschließend auf "Entschlüsseln".

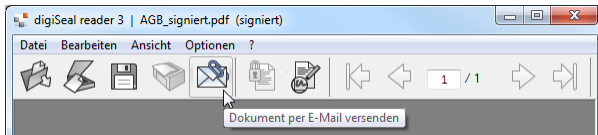


3. Bei korrekter Eingabe wird die Datei entschlüsselt und je nach Format im Secure Viewer Fenster oder im Dateimonitor geöffnet. Die entschlüsselte Datei kann anschließend an einem beliebigen Ort abgespeichert werden.

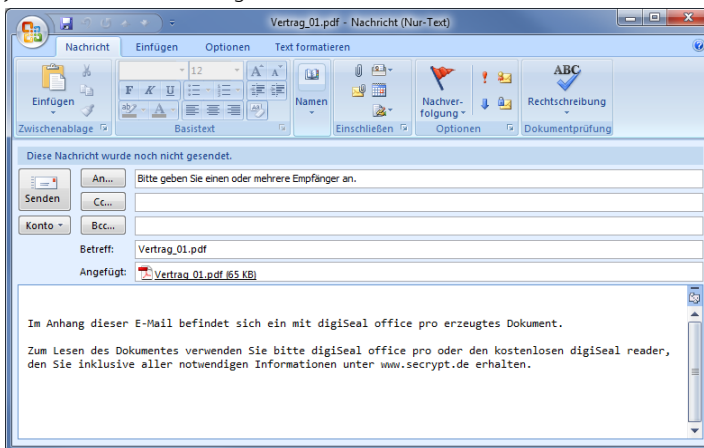
4.2. E-Mail-Versand

Ein Dokument kann direkt aus dem digiSeal® reader heraus im Anhang einer E-Mail versendet werden.

1. Das zu versendende Dokument ist im digiSeal® reader geöffnet. Bevor Sie es per E-Mail versenden können, muss es abgespeichert werden.
2. Betätigen Sie die Schaltfläche "Dokument per E-Mail versenden" oder »Datei / Senden an...«.



3. Es öffnet sich eine neue E-Mail in Ihrem (Standard-) E-Mail-Client mit dem Dokument im Anhang.
4. Jetzt können Sie wie gewohnt Ihren Text schreiben und die E-Mail versenden.



Hinweis: Achten Sie darauf, dass in Ihrem E-Mail-Client ein E-Mail-Konto eingerichtet ist. Andernfalls ist ein Versand nicht möglich.