

PRESSE-INFORMATION



soft Xpansion veröffentlicht *Smart Card Crypto Provider 3* – die Software-Bibliothek für sichere digitale Unterschriften

(Bochum, 26. Mai 2008) - Eine digitale Unterschrift ersetzt beim Unterzeichnen von Dokumenten die eigenhändige Unterschrift auf Papier. An die Stelle von Papierdokumenten treten dann elektronische Dokumente, zum Beispiel PDF-Dateien. Die digitale Unterschrift kann unter Verwendung eines handelsüblichen PCs, der entsprechenden Software und zusätzlicher Hardware, wie zum Beispiel einer Kombination aus Smart Card und Lesegerät, erfolgen. Der technische Prozess des digitalen Unterzeichnens ist allerdings eine komplizierte Aufgabe, die speziell für diesen Zweck programmierte Software erfordert. Darüber hinaus verfügt fast jede Smart Card über ihre eigenen, spezifischen Eigenschaften, was zusätzlichen Aufwand für die erforderliche Softwareanpassung bedeutet.

Smart Card Crypto Provider 3 – schnell & sicher digital unterschreiben
Die Smart Card Crypto Provider-Bibliothek von soft Xpansion erleichtert die Implementierung von digitalen Unterschriften in Geschäftsprozesse. Sie vereinfacht die Verwendung von Smart Card-Zertifikaten für die Ver- und Entschlüsselung. Tiefer gehende Kenntnisse über die technischen Abläufe beim digitalen Unterzeichnen von Dokumenten benötigt der Software-Entwickler mit diesem Produkt nicht. Die Bibliothek kann schnell und mit geringem Aufwand mit Software-Anwendungen verknüpft werden. Die Verschlüsselung/Entschlüsselung erfolgt über die von Microsoft® für Programmierer zur Verfügung gestellte Verschlüsselungs-Applikations-Schnittstelle, die „Crypto API“. Außer den installierten Hardwaretreibern, zum Beispiel für das Kartenlese-Gerät, sind keine weiteren Komponenten erforderlich. Es können alle Kartenleser verwendet werden, die den PC/SC-Standard unterstützen.

Die wichtigsten Funktionen:

- Voll kompatibel mit Microsofts Crypto API
- **NEU:** Unterstützung von RSA (PKCS#1)- und ECC (PKCS#13)-Algorithmen
- Unterstützung von Smart Cards und eTokens entsprechend den PKCS#11- und PKCS#15-Standards
- **NEU:** Unterstützung von zwei Modi zur PIN-Eingabe: neben Eingabe über Tastatur und Software-GUI jetzt auch direkt über PIN-Pad
- Unterstützung von PC/SC-kompatiblen Lesegeräten
- **NEU:** jetzt auch kompatibel mit Smart Cards der Aladdin eToken-Familie

Unterstützte Smart Cards:

Die Bibliothek ist mit den in Deutschland und Europa gängigsten Smart Cards verwendbar. Diese sind gegenwärtig

- T-TeleSec E4NetKey V2.0-Karte
- Deutsche Post SIGNTRUST-Karte
- Deutsche Bank db SignaturCard
- D-TRUST Standard-Signaturkarte
- S-TRUST SparkassenCard
- A-TRUST a.sign
- Aladdin eToken-Familie

Produktübersicht:

Details zu *Smart Card Crypto Provider 3* finden sich auch auf der [Produktseite](#) im Internet.

Download:

Für *Smart Card Crypto Provider 3* kann [hier](#) die Demo-Applikation *PDF Quick Reader 4* (Freeware) herunter geladen werden. *PDF Quick Reader 4* verwendet die Smart Card Crypto Provider-Bibliothek, um PDF-Dokumente mit Zertifikaten zu unterzeichnen, die lokal auf dem Rechner, auf Smart Cards oder auf USB-Sticks gespeichert sind. Im Programm-Menü ist die implementierte Bibliothek über *Dokument/Signieren...* zugänglich.

Betriebssysteme:

Die Bibliothek unterstützt alle aktuellen Windows-Plattformen: Windows® Vista, XP, Server 2003, 2000.

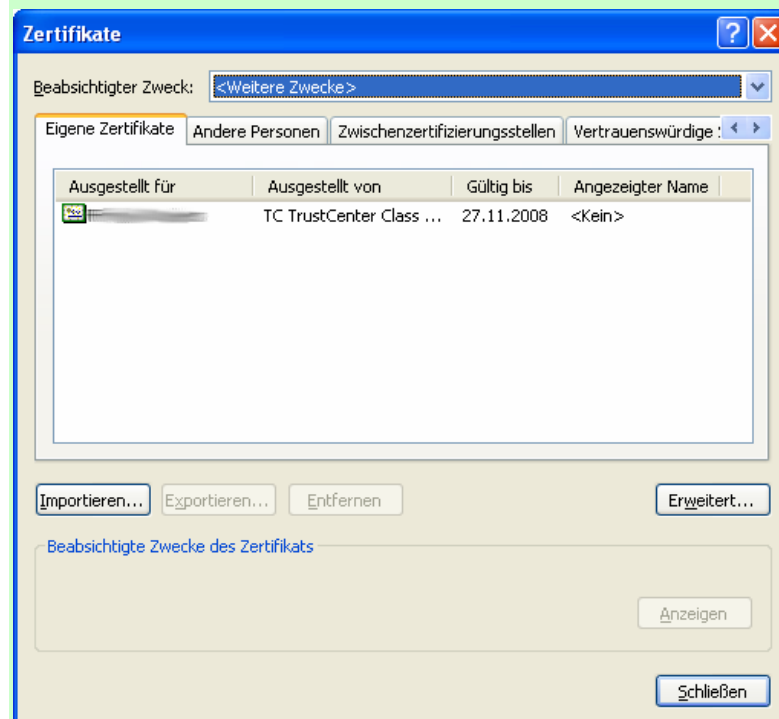
Abbildungen & Screenshots:

Demo-Screenshots finden sich im nachfolgenden Beispiel. Sie können auch als separate Bilddateien unter pr@soft-xpansion.com angefordert werden. Die Abbildungen stammen aus dem Internet Explorer 7 und aus *PDF Quick Reader 4*.

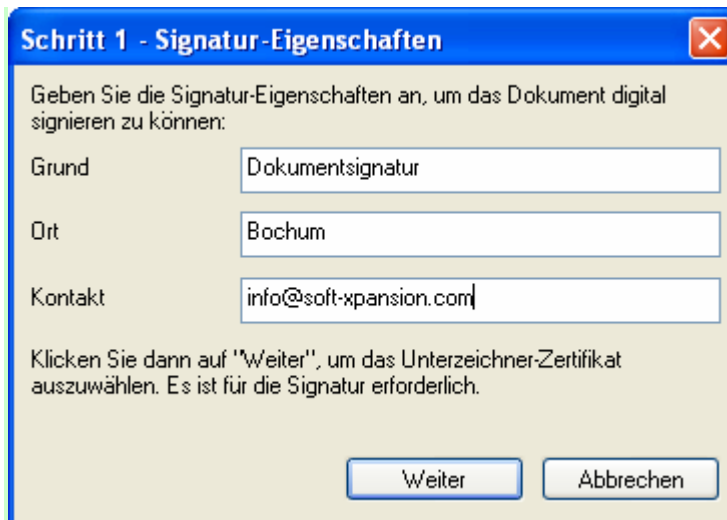
Hintergrundinformationen:

Im weiterführenden Fachartikel „[Smartcards und ihre Rolle in der Zwei-Faktoren-Authentifizierung](#)“ werden die Einsatzmöglichkeiten von Smart Cards bei der Überprüfung von Zugangs- und Zugriffsberechtigungen beleuchtet.

Beispiel - implementierte Smart Card Crypto Provider 3-Bibliothek:



Ansicht der auf dem Computer gespeicherten Zertifikate (Menü *Extras/Internetoptionen/Inhalte/Zertifikate*) im Internet Explorer 7



Schritt 1 - Signatur-Eigenschaften

Geben Sie die Signatur-Eigenschaften an, um das Dokument digital signieren zu können:

Grund: Dokumentsignatur

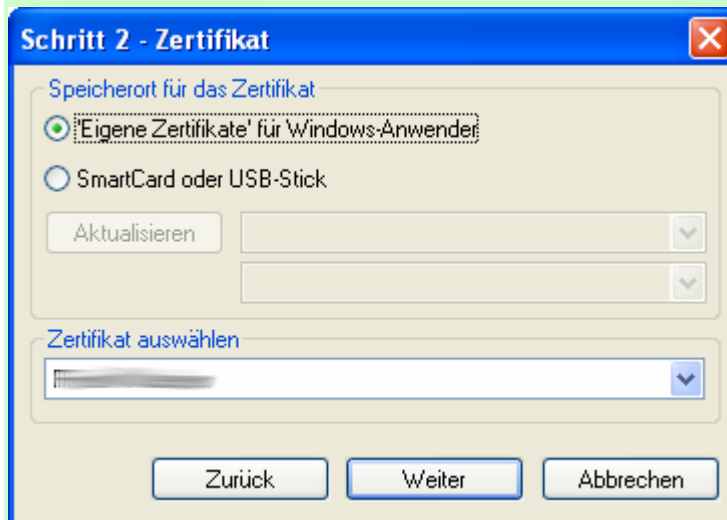
Ort: Bochum

Kontakt: info@soft-xpansion.com

Klicken Sie dann auf "Weiter", um das Unterzeichner-Zertifikat auszuwählen. Es ist für die Signatur erforderlich.

Weiter Abbrechen

Auswahl der Signatur-Eigenschaften



Schritt 2 - Zertifikat

Speicherort für das Zertifikat

☒ Eigene Zertifikate für Windows-Anwender

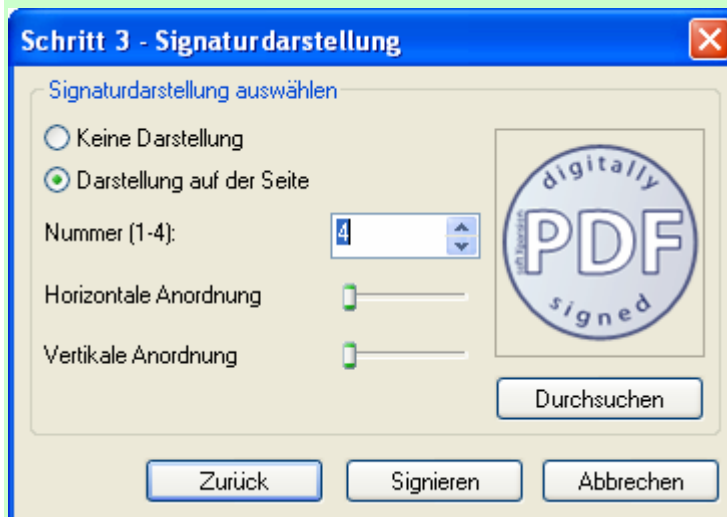
☐ SmartCard oder USB-Stick

Aktualisieren

Zertifikat auswählen

Zurück Weiter Abbrechen

Auswahl des Zertifikats



Schritt 3 - Signaturdarstellung

Signaturdarstellung auswählen

☐ Keine Darstellung

☒ Darstellung auf der Seite

Nummer (1-4): 4

Horizontale Anordnung

Vertikale Anordnung

Durchsuchen

Zurück Signieren Abbrechen

Festlegung der Darstellung der Signatur im Dokument

PDF Quick Reader 4.0

Das angegebene Dokument wird jetzt unterschrieben.
Soll das Zertifikat "i:..." für die Unterschrift verwendet werden?

Digitale Unterschrift des Dokuments mit dem Zertifikat

Digitale Signaturen_1_kurz.pdf - PDF Quick Reader 4.0

Datei Bearbeiten Ansicht Dokument Werkzeuge Fenster Hilfe

3. Signieren im PDF-Format

Grundsätzlich kann jedes elektronische Dokument digital unterschrieben werden und es besteht die Möglichkeit, die Unterschriften zu verifizieren. Ein elektronisches Dokument ist normalerweise eine separate Datei oder ein Datensatz in einer Datenbank. Aber auch die digitale Signatur selbst ist ein Datensatz der gespeichert werden muss. Nicht alle Dateiformate erlauben es, „freier“ Daten – was elektronische Signaturen aus Sicht der eigentlichen Dokumente sind – in das Dokument zu integrieren. In diesen Fällen muss die Signatur als eine separate Datei immer zusammen mit dem Dokument versandt und aufbewahrt werden.

Einige Dateiformate erlauben hingegen die direkte Integration von digitalen Signaturen, und zwar Adobe's PDF und Microsofts XPS oder XML-basierte Formate. Da sich das PDF-Format erstens als Quasi-Standard für den Austausch und für die Archivierung von elektronischen Dokumenten etabliert hat (XPS ist ein noch relativ junges Format) und da es zweitens speziell für den Bereich der digitalen Signaturen gesonderte Spezifikationen bereit hält, wird PDF für das elektronische Signieren in der Praxis immer häufiger verwendet.

Das PDF-Format bietet flexible und vielfältige Möglichkeiten, die eine Verwendung von digitalen Signaturen sowohl für den Softwareentwickler als auch für den dem Anwender attraktiv machen. Wie eine einzelne digitale Signatur in einer PDF-Datei verankert wird zeigt Abbildung 3a.

PDF-Datei mit einer Signatur

Dateistruktur	Byte
PDF-Körper	0
Byteränge	650
Contents	0.650.000.1200
Signaturinhalt	
Weitere Attribute	
PDF-Körper (Erweiterung)	800
	1200

PDF-Datei mit mehreren Signaturen

Dateistruktur	Byte
PDF-Körper	0
Byteränge	650
Contents	0.650.000.1200
Signaturinhalt	
Weitere Attribute	
PDF-Körper (Erweiterung)	800
Update1	1400
Byteränge	0.1400.000.2000
Contents	
Signaturinhalt	
Weitere Attribute	
Update1 (Erweiterung)	1600
	2000

Abbildungen 3 a) und b)

Das ByteRange-Attribut definiert, welcher Inhalt der PDF-Datei durch eine so genannte Hashfunktion verschlüsselt werden soll. Dies ist üblicherweise der komplette Inhalt der Datei oder der Nachricht, mit Ausnahme der Signatur selbst. Die Hashfunktion ist ein mathematisches Verfahren, mit dem eine Nachricht oder ein Dokument in einen Zahlenwert als Kurzfassung umgerechnet wird. Das Contents-Attribut der PDF-Datei beinhaltet die wichtigsten Signaturbestandteile wie den Hashwert und den öffentlichen Schlüssel. Weitere Attribute sind spezielle technische Eigenschaften, die in der PDF-Spezifikation von Adobe beschrieben sind und vom Softwareentwickler berücksichtigt werden müssen.

Die Signatur in der PDF-Datei kann zum einen eine komplett vom System berechnete, rein mathematisch erstellte Signatur sein. Sie kann aber auch auf biometrischen Merkmalen wie einer handschriftlichen Signatur, einem Fingerabdruck oder einem Scan der Netzhaut basieren. Dabei sollte es so sein, dass PDF-Produkte für Anwender die Zusammenarbeit von unterschiedlichen Signaturprogrammen erlauben: eine mit einer Anwendung 1 des Verfassers 1 signierte PDF-Datei muss mit einer anderen Anwendung 2 eines anderen Verfassers überprüfbar sein.

Abbildung 3b zeigt schematisch die Struktur einer mehrfach signierten PDF-Datei.

Mehrfachsignaturen im PDF-Dokument können mittels so genannter inkrementeller Updates realisiert werden. Inkrementelle Updates fügen alle Modifikationen an das Ende der Datei an, so dass die ursprünglichen Daten unberührt bleiben. Somit ist es relativ einfach, einzelne oder alle Updates rückgängig zu machen, um eine bestimmte Dateiversion zu erhalten. Und im Falle von mehrfach signierten Dokumenten kann man so sowohl die originalen Inhalte der Person, die zuvor signiert hat als auch seine eigenen Vermerke (das Update) signieren und damit bestätigen.

4. Vertraulichkeit von Informationen durch die digitale Signatur?

Wie bereits erwähnt können bei einer elektronisch signierten E-Mail oder PDF-Datei die Identität des Verfassers und die Integrität der Nachricht überprüft werden. Dies bedeutet jedoch nicht automatisch, dass auch die Nachricht selbst so verschlüsselt wird, dass Unbefugte sie nicht lesen können. Vielmehr wird in der Regel die unverschlüsselte Originalnachricht neben der Signatur, dem Zertifikat und dem Hashwert der Nachricht übermittelt. Moderne Software-Produkte bieten deshalb zusätzliche Funktionen, mit denen auch die Nachricht selbst verschlüsselt werden kann.

5. Rechtliche Grundlagen

Den rechtlichen Rahmen für die Verwendung digitaler Signaturen bilden im Wesentlichen:

- EG-Richtlinie 1999/93/EG (Signaturrichtlinie)
- Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG)
- Rahmenwerk „Einheitliche Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponenten“
- Verordnung zum Signaturgesetz (SigV)
- Bürgerliches Gesetzbuch
- Zivilprozessordnung

Das digital signierte Dokument

Über soft Xpansion:

soft Xpansion ist ein weltweit tätiges internationales Team, das seit seiner Gründung im Jahr 1995 über 100 Software-Produkte entwickelt hat. Die Absatzmärkte sind außer Deutschland, Österreich und der Schweiz eine Vielzahl weiterer Länder, in denen lokalisierte Produktversionen veröffentlicht werden. Hierzu zählen unter anderem Großbritannien, Frankreich, Italien, die USA, die Beneluxländer, die Ukraine, Spanien, Russland, Portugal, Australien und die Türkei. soft Xpansion bietet Lösungen (Individualentwicklung, Entwickler-Bibliotheken, Standardsoftware und Freeware), die auf die Bereiche PDF-Technologie, Dokumenten- und Datenbank-Managementsysteme sowie Daten- und Anwendungssicherheit fokussiert sind. Weitere Informationen zum Unternehmen finden Sie im Internet unter <http://www.soft-xpansion.de>. soft Xpansion ist Mitglied im PDF/A Competence Center, <http://www.pdfa.org>.

Kontakt:

soft Xpansion GmbH & Co. KG, Frank Dückers, Königsallee 45, 44789 Bochum
Tel.: +49 234 298 41 71 Fax: +49 234 298 41 72

E-Mail: dueckers@soft-xpansion.com