

# CryptLib y

Kryptographie API  
für verschiedene  
Plattformen



**XPS** Software GmbH

Cross Platform Solutions

Wir verbinden Welten



## Die Highlights

Verfügbar für Win32, Linux, OS/2, OS/400 (iSeries), VSE/ESA, z/VSE, MVS/ESA, OS/390, z/OS (zSeries)

Erstellung von RSA Schlüsselpaaren mit bis zu 4096 Bit Schlüssellänge

Asymmetrische Verschlüsselung mit der RSA Methode

Symmetrische Verschlüsselung mit AES, DES, TripleDES, RC2, RC4 und Blowfish

Digitale Signatur mit RSA in Kombination mit den Hashfunktionen MD2, MD5, SHA-1, SHA-256, SHA-386, SHA-512, RipeMD160

Verarbeitung von X.509 Zertifikaten

Erzeugung und Verarbeitung von S/MIME Objekten (PKCS#7)

Verarbeitung von PKCS#12 Objekten zum Austausch von Schlüsseln und Zertifikaten

ISIS-MTT kompatibel

## Die Herausforderung

Die Kryptographie übt seit jeher eine große Faszination auf die Menschen aus. Die Vorstellung, Informationen so zu chiffrieren, dass eine Dechiffrierung durch eine andere Partei nur unter Kenntnis eines bestimmten Geheimnisses möglich ist, eröffnet viele interessante Perspektiven.

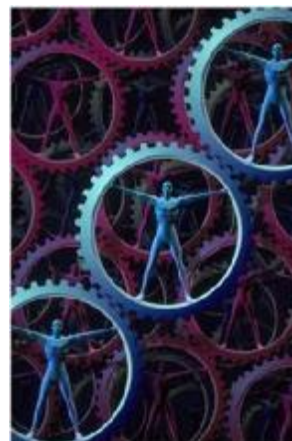
Historisch betrachtet kann man die Anfänge der Kryptographie bis in das 19. Jahrhundert vor Christus verfolgen. Seitdem hat sie auf vielen Gebieten eine wichtige Rolle gespielt, wobei sicherlich militärische und geheimdienstliche Motive entscheidend für den überwiegenden Teil der Entwicklung waren.

Die großen Fortschritte sowohl auf dem Gebiet der Mathematik als auch im Bereich von Computer Hardware und die Verbreitung des Internet machen die 'Kryptographie' zunehmend auch für andere Benutzergruppen zugänglich und effektiv nutzbar.

## Das Problem

Obwohl auf dem Gebiet der Kryptographie enorme Fortschritte gemacht wurden, erschließt sich das Thema selbst interessierten Anwendern eventuell nur sehr schwer. Das liegt vor allem darin begründet, dass die Kryptographie zum einen auf durchaus komplizierten mathematischen Grundlagen basiert und zum anderen die Verfahrensweisen zur Nutzung der Kryptographie, die sich als Standards etabliert haben, nicht trivial sind.

Des weiteren ist der Schritt vom reinen Verständnis eines kryptographischen Zusammenhangs hin zu einer Software basierten Implementierung, die dessen Nutzung effektiv ermöglicht, für viele nicht gangbar. Das begründet sich vor allem am variablen und komplizierten Aufbau kryptographischer Strukturen, deren Format im allgemeinen gemäß der Abstract Syntax Notation One (ASN.1) beschrieben ist.



Dennoch entsteht natürlich in vielen Situationen ein konkreter Bedarf am Einsatz von Kryptographie. Und überall dort, wo dieser nicht über Standards, die bereits in der eingesetzten Software integriert sind, abgedeckt wird, sind weitere Schritte erforderlich. Wünschenswert wäre daher ein Softwarepaket, das sowohl günstig ist aber dennoch das breite Spektrum der denkbaren kryptographischen Funktionen abdeckt und möglichst einfach in eigene Programme eingebunden werden kann. Weiterhin wäre die Verfügbarkeit des Pakets auf verschiedenen Plattformen wünschenswert. CryptLib von der XPS Software GmbH erfüllt diese Anforderungen.

## Die Lösung

### CryptLib - Kryptographie API für verschiedene Plattformen

CryptLib von der XPS Software GmbH ist eine Programmierschnittstelle, die die Einbindung einer Vielfalt an kryptographischen Funktionen in selbst entwickelte Software ermöglicht. XPS bietet CryptLib-Versionen für die folgenden Betriebssysteme an: Win32, Linux, OS/2, OS/400 (iSeries), VSE/ESA, z/VSE, MVS/ESA, OS/390, z/OS (zSeries). Speziell im IBM-Großrechnerbereich stellt CryptLib von XPS eine sehr interessante Alternative zu verfügbaren Hardwarelösungen dar.



### Einweg-Hashfunktionen

Hashfunktionen spielen bei vielen Sicherheitsverfahren eine bedeutende Rolle, da sie als eindeutiger Repräsentant einer beliebig langen Nachricht verwendet werden können. Sie kommen z. B. bei der Integritätsprüfung von Daten zum Einsatz. CryptLib unterstützt die folgenden Hashfunktionen: MD2, MD5, SHA-1, SHA-256, SHA-386, SHA-512 und RipeMD160.

### Verschlüsselung

Verschlüsselung wird zur Gewährleistung der Vertraulichkeit von Daten eingesetzt. Dazu wird der Klartext durch Anwendung eines offen gelegten mathematischen Verfahrens unter Verwendung eines geheimen Schlüssels in eine nicht lesbare Form transformiert, die es einem Angreifer idealer Weise unmöglich macht, die Originaldaten ohne Kenntnis des verwendeten Schlüssels zu rekonstruieren. Man unterscheidet symmetrische und asymmetrische Verfahren. Bei symmetrischen Verfahren wird der gleiche Schlüssel zum Ver- und Entschlüsseln verwendet. Bei asymmetrischen Verfahren sind die Schlüssel zum Ver- und Entschlüsseln verschieden. Man spricht in diesem Fall auch von so genannten Public-Key-Verfahren. CryptLib unterstützt die folgenden symmetrischen Verfahren: AES, DES, TripleDES, RC2, RC4 und Blowfish. Aus dem Bereich der asymmetrischen Verschlüsselung unterstützt CryptLib das RSA-Verfahren.

### Zertifikate

Zertifikate sind elektronische Ausweise, die im Zuge der Erfindung von Public-Key-Verfahren entwickelt wurden. Neben spezifischen Informationen über den Inhaber des Zertifikats enthält ein Zertifikat einen öffentlichen Schlüssel und Informationen über den Aussteller, bzw. über die gesamte Ausstellerkette. Durch Zurückverfolgung der Ausstellerkette bis zu einem als vertrauenswürdig eingestuftem Aussteller kann die Richtigkeit und Gültigkeit des Zertifikats sichergestellt werden. CryptLib unterstützt die Verwendung von digitalen X.509 Zertifikaten.

### Public Key Cryptography Standards

Unter den verschiedenen PKCS#-Kürzeln stellen die RSA-Laboratorien eine Reihe von Standardspezifikationen im Umfeld der Kryptographie zur Verfügung. CryptLib unterstützt die Verwendung von PKCS#12 und PKCS#7.

PKCS#12 (Personal Information Exchange Syntax Standard) bezeichnet eine Syntax für den Austausch von Schlüsseln und Zertifikaten. Die Informationen in einem PKCS#12 Objekt sind entweder über eine asymmetrisches Verschlüsselungsverfahren oder durch ein Passwort geschützt und können nur von Personen, die das entsprechende Geheimnis kennen, dechiffriert und gelesen werden.

PKCS#7 (Cryptographic Message Syntax Standard) beschreibt eine Syntax, nach der Daten durch kryptographische Maßnahmen wie digitale Signaturen oder Verschlüsselung geschützt werden können. Das vermutlich bekannteste Einsatzgebiet von PKCS#7 ist S/MIME, ein Verfahren zur Verschlüsselung und zum Signieren MIME-gekapselter elektronischer Post (hauptsächlich E-Mail).

### SSL/TLS (Secure Sockets Layer / Transport Layer Security)

SSL/TLS erlaubt die Verschlüsselung von Daten auf der Ebene des Netzwerkprotokolls. In Begriffen des OSI-Modells findet die Ver- und Entschlüsselung zwischen Transport- und Anwendungsschicht statt. Damit arbeitet SSL/TLS anwendungstransparent und kann zur Sicherung von primär nicht gesicherten Netzwerkanwendungen eingesetzt werden. Das bekannteste Beispiel für den Einsatz von SSL/TLS ist HTTPS zur Sicherung von Informationen, die über das Internet ausgetauscht werden. CryptLib unterstützt das SSL/TLS-Verfahren durch die Bereitstellung von SSL/TLS Sockets für die Kommunikation über TCP/IP.

## Weitere Produkte der XPS Software GmbH

### ServEx - Standardkonforme Web Services für IBM Mainframes - SOA

- Kapselung beliebig komplexer Host Prozesse mit Zugriff über XML/SOAP (Java Servlet)
- XML basierte Ausführung von 3270 Transaktionen
- Bereitstellung originaler 3270 Feldnamen für CICS/BMS, IMS/MFS und CA-Ideal
- XML basierte Ausführung von Commarea Transaktionen unter CICS, IMS und MVS/Batch
- Datenaustausch für Commarea Transaktionen über originale Cobol und PL/1 Datenstrukturen

### JProtector - Java 3270/5250 Terminal- und Druckeremulation

- Web-to-Host fähig (Browser-basiert als Java-Applet oder über Java-Webstart)
- Programmierung über JavaBeans, OHIO (Java) und EHLLAPI (Win32)
- bei Bedarf Authentisierung, Verschlüsselung und Komprimierung
- Generierung von HTML on-the-fly

### PrintEx - IBM Mainframe Print Services Extender

- Ausdruck auf TCP/IP-Drucker über LPR/LPD oder direct sockets
- Umleitung der Druckausgabe von VTAM-Applikationen (z. B. CICS, IMS) nach JES
- Versenden der Druckdaten per E-Mail als PDF-Anhang
- Konvertierung der Ausgabedaten nach Postscript oder PCL
- Formulardruck durch die Einbindung externer Grafiken als Overlays
- Drucken von Barcodes
- Optionale ThinPrint Server Engine Host

### Transit - Windows Druckserver

- Verteilung von LPD-Druckdaten an lokale Drucker und an Netzwerkdrucker
- Einbindung externer Grafiken in Druckausgaben beliebiger Programme wie z. B. MS-Word (Formulardruck)
- Implementierung des LPD-Protokolls über SSL/TLS
- Automatisiertes Versenden von Daten über FTP/FTPS
- Komprimierung der übertragenen Daten mittels ZIP

### RACFBroker - programmierbarer Zugriff auf RACF/Mainframe

- Java- und Win32-Programmierschnittstellen
- Bereitstellung von RACF-Funktionen für Netzerkanwendungen
- vollständig end-to-end verschlüsselte Datenübertragung

## Kontakt

XPS Software GmbH

Untere Hauptstr. 2  
D-85386 Eching

Fon +49-(0)89-456989-0  
Fax +49-(0)89-456989-29  
Mail [info@xps.biz](mailto:info@xps.biz)  
Web <http://www.xps.biz>

Alle Rechte sowie technische Änderungen vorbehalten.  
Verwendete Firmen-, Hard- und Softwarenamen sind anerkannte  
Handelsnamen und/oder Marken der jeweiligen Hersteller.  
Copyright © XPS Software GmbH