CryptLib

Cryptography API For Various Platforms

XPS Software GmbH
Cross Platform Solutions
dare to be sophisticated

CryptLib

CryptLib - Cryptography API for various platforms

CryptLib from XPS is an application programming interface that can be used to include a variety of cryptographic functions in self developed software programs. CryptLib is available for the following operating systems:

Win32
Linux
OS/400 (IBM iSeries)
z/VSE
z/OS

Highlights

Available on Win32, Linux, OS/400 (IBM iSeries), z/VSE, z/OS (IBM zSeries)

Generation of RSA key pairs with up to 4096 bit key length

Asymmetrical encryption using RSA

Symmetrical encryption using AES, DES, TripleDES, RC2, RC4 and Blowfish

Digital signatures with RSA in combination with MD2, MD5 and SHA 1 hash methods, SHA-256, SHA-386, SHA-512, RipeMD160

Processing of X.509 certificates

Generation and processing of S/MIME objects (PKCS#7)

Processing of PKCS#12 objects for the exchange of secret keys and certificates

ISIS-MTT compatible

Encryption

Encryption is used to guarantee the confidentiality of data. In order to do so plaintext is transformed into a non readable format by applying a disclosed mathematical procedure using a secret key. Ideally it's impossible for an offender to reproduce the original data from the encryption result without the knowledge of the secret key that has been used.

A distinction is drawn between symmetrical and asymmetrical encryption methods. Symmetrical encryption methods use an identical key for encryption and decryption. On the other hand the keys used for encryption and decryption are different when using asymmetrical encryption. The latter is also known as Public-key cryptography.

CryptLib supports the following symmetrical methods:

AES (Rijndael)
DES
TripleDES
RC2
RC4
Blowfish

From the area of Public-key cryptography RSA is supported by CryptLib.

One-way hash methods

Hash methods are of great importance in many security procedures. This is due to the fact that a hash value can be used as a unique representative of a message of arbitrary length. Hash values are used, among others, in the area of integrity checks. CryptLib supports the following hash methods:

MD2, MD5
SHA-1, SHA-256, SHA-386, SHA-512
RipeMD160

Certificates

Certificates are electronic identification cards having been developed during the invention of Public-key cryptography. Besides specific information about the owner, a certifcate contains a public key as well as information about the issuer respectively the chain of issures of the certificate. Backtracking the chain of issuers up to an issuer estimated as confidential, the accuracy and validity of a certificate can be assured.

CryptLib supports the use of standard X.509 digital certificates.

Public-key cryptography standards

Using various PKCS#-acronyms, RSA laboratories provide a number of standard specifications in the area of cryptography. CryptLib supports the explicit use of PKCS#12 and PKCS#7.

PKCS#12 (Personal Information Exchange Syntax Standard) describes a syntax for the exchange of keys and certificates. Information stored in a PKCS#12 object are either protected using an asymmetric encryption method or using a password. Thus the information stored can only be deciphered and read by entities knowing the secret used to seal the PKCS#12 object.

PKCS#7 (Cryptographic Message Syntax Standard) describes a syntax used to protect information using cryptographic procedures such as digital signatures or data encryption. S/MINE is probably the best known application of PKCS#7. S/MIME is used to encrypt and sign MIME-encapsulated electronic post (mainly e-mail).

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

SSL/TLS is used to encrypt and decrypt data on the network protocol layer. In terms of the OSI model, encryption and decryption are carried out between the transport- and the application layer. This implicates that SSL/TLS works transparently in relation to application programs and thus can be used to secure formerly not secured network applications. The best known example for the use of SSL/TLS is HTTPS used to secure information exchanged via the internet.

CryptLib

More Products from XPS Software GmbH

Host Connectivity

JProtector - Programmable Java 3270/5250 Terminal and Printer Emulation

- Web-to-Host enabled
- Programmable using JavaBeans, OHIO (Java) and EHLLAPI (Win32)
- Remote host access over TCP/IP port 80 (Fireproof)
- Authentication, strong encryption and compression on demand

Printing

PrintEx - IBM Mainframe Print Services Extender

- Extended printing facilities for IBM z/OS and z/VSE
- Output on TCP/IP printers via LPR/LPD or direct sockets
- Dispatching print output as a PDF-attachment via e-mail
- On the fly data conversion to Postscript or PCL

File Transfer

HostDrive - Automated Multi Platform File Transfer

- Available for z/OS, z/VSE and for all platforms providing a Java Virtual Machine
- Delivery guarantee
- Direct reading and writing of VSAM/KSDS and VSAM/ESDS
- Support for FTP, LPD, JMS and e-mail on Java platforms

Contact

XPS Software GmbH
Mühlanger 7
D-85777 Fahrenzhausen

Fon +49-(0)89-456989-0
Fax +49-(0)89-456989-19
Mail info@xps.biz
Web www.xps-software.com