Entrust® Alliance

Entrust/Toolkit™

Java™ Edition

What is Entrust/Toolkit™ Java™ Edition?

Designed specifically for Java developers, Entrust/Toolkit™ Java™ Edition is a fast, cost-effective way to build SSL, PKIX, PKCS #7 and Entrust-Ready™ security applications.

Implemented entirely in the Java programming language, this powerful toolkit enables developers to easily add flexible, modular security services for hashing, encrypting and signing with X.509 certificates. Unlike other products, it supports multiple CA vendors including the Entrust/PKI™, the only Managed PKI for securing enterprise information and is available at absolutely no cost to developers at developer.entrust.com

Entrust/Toolkit Java Edition provides both high and low-level application programming interfaces (APIs) for performing cryptographic operations. It is not an application, but a set of APIs called by other Java code to perform security-related tasks. It is implemented completely in Java with no reliance on native code and it adheres to the Java Security Architecture and supplements the Java Cryptography Extension (JCE) with numerous cryptographic algorithms.

Features and benefits

Fully scalable

Entrust's full security system is scalable to address even the most demanding requirements of an organization. With Entrust, developers can start with individual users or small workgroups and grow to suit the needs of any size organization.

Algorithm independent

In the case of Entrust/Toolkit Java Edition, algorithm selection is made available through the JCE Module providing RSA, DSA, SHA1, MD5, MD2, DES, Triple-DES, CAST-128, RC2 and RC4 algorithms.

Seamless integration

Applications developed with this toolkit have the option of tying seamlessly into the Entrust/PKI through the use of API calls designed to create or use Entrust user credentials. These applications are thus able to co-exist with other Entrust-Ready applications sharing the same credentials, thus conforming to the concept of the "single security architecture"

Flexible

Entrust/Toolkit Java Edition offers Multiple levels of APIs for both high and low-level cryptographic programming.

Interoperable

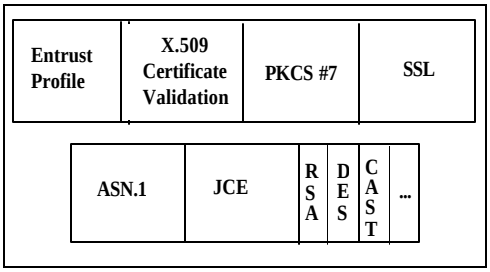
Since implementation is completely in Java, all Java environments, including browsers and Network Computers, are supported.

Entrust/Toolkit Java Edition Capabilities

· Supports the use and management of Entrust user credentials,
· Full certificate life-cycle management and support for PKIX-based protocols,
· Full X.509 Version 3 certificate and chain validation,
· Creates and processes PKCS#7 enveloped messages,
· Secure Socket Layer (SSL) version 3 connections to and from Java applets or applications.

Architecture

The Entrust/Toolkit Java Edition has a modular architecture.



Each module has its own API which are as follows:

· **Java Cryptographic Extension (JCE) Module** provides RSA, DSA, SHA1, MD5, MD2, DES, Triple-DES, CAST-128, RC2 and RC4 algorithms.

· **Generic ASN.1 Module** provides encoding and decoding with the numerous X.509 structures (including certificates, standard extensions, CRLs).

· **Entrust Profile Module** provides creation, usage and updating capabilities.

· **X.509 Certificate Validation Module** supports PKI networking, certificate revocation checking and X.509 Version 3 standard extension verification.

· **PKCS #7 Module** provides encoding and decoding of this standard enveloping format for encrypted and/or digitally signed data.

· **SSL Module** provides the most frequently used method of secure TCP/IP communications on the Internet.

System requirements

The Entrust/Toolkit Java Edition is designed to work in a Java environment that provides full implementations of either JDK 1.1 or 1.2. Javasoft's Java Plugin may be used to provide JDK 1.1 compliance to Internet Explorer 3.02 and later, and Netscape Navigator 3.0 and later, Java environments.

Algorithm support

Message digests
- md2 128
- md5 128
- sha1 160

Signature
- md2WithRSA
- md2WithDSA
- sha1WithRSA
- sha1WithDSA
- md5WithRSA

Password- based encryption
- pbeWithMD5AndDES_CBC
- pbeWithSHAAndDES_CBC
- pbeWithSHAAndRC240_CBC
- pbeWithSHAAndCast5_CBC

Public key
- RSA 512,1024,2048
- DSA 512,1024
- Diffie-Hellman 512,1024,2048

Secret key
- DES 56
- Triple DES 168
- CAST5 40-128
- RC2 40-128
- RC4 40-256

For more information on Entrust/Toolkit, call us at:

(888-690-2424) or
(613-247-3411) or

visit our Web site at
developer.entrust.com