



**Securing Your
Digital Life**

Entrust Authority Toolkit Overview

December 2007

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. Entrust is a registered trademark of Entrust Limited in Canada. All other company and product names are trademarks or registered trademarks of their respective owners. The material provided in this document is for information purposes only. It is not intended to be advice. You should not act or abstain from acting based upon such information without first consulting a professional. ENTRUST DOES NOT WARRANT THE QUALITY, ACCURACY OR COMPLETENESS OF THE INFORMATION CONTAINED IN THIS ARTICLE. SUCH INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATIONS AND/OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, AND/OR WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT, OR FITNESS FOR A SPECIFIC PURPOSE.

Copyright © 2006. Entrust. All rights reserved.

Entrust Authority Toolkit Overview

Entrust offers a selection of software development kits (toolkits) for adding security to applications. These applications could be custom applications developed by Entrust customers, applications developed by partners of Entrust, or even products offered from Entrust.

The toolkits can be used to integrate with, and take advantage of, other Entrust products (e.g., PKI) or to add security independent of any specific Entrust products.

The various toolkits provided by Entrust cover a wide range of security capabilities, development languages and operating platforms. This document will enumerate the various Entrust toolkits and describe their purpose and general functionality. Detailed documentation is available for a more thorough understanding of each toolkit.

Toolkit Description

Java Security Toolkits

The Security Toolkit for the Java Platform is a feature-rich toolkit for adding various security features to your Java applications. This is Entrust's most popular toolkit due to the toolkit's flexibility, standards conformance, portability, and its high performance characteristics. It can be used to serve a wide range of application requirements.

Some of the general capabilities of the Security Toolkit for the Java Platform include:

- FIPS 140-2 validated cryptographic engine (with wide variety of cryptographic algorithms)
- SSL/TLS (both client and server)
- Data encryption & decryption (e.g., PKCS#7/CMS, XML, S/MIME)
- Digital signature creation & verification, certificate path validation
- Key and certificate management (create, request, renew, recover, protect, etc.)

The Security Toolkit for the Java Platform complies with all relevant standards and has received important third-party validations (e.g., FIPS, PKITS). The flexibility of this toolkit is unsurpassed:

- High-level APIs available to reduce development time. Low-level APIs for greater control.
- Works with or without a PKI. Works with Entrust PKI or non-Entrust PKI.
- Modular design allows you to pick and chose only the components you need.
- Huge selection of standards-based cryptographic algorithms and mechanisms.

Also available is a special version of this toolkit for the IBM Z-series platform: Security Toolkit z/OS Edition for the Java Platform. This toolkit has the same rich feature set as the “regular” version.

PKI Administration Toolkits

The PKI administration toolkits provide programmatic access to various administrative functions for the Entrust PKI server: Entrust Authority Security Manager. By using these toolkits, one could build an application which managed all administrative aspects of the Entrust PKI, including policies, users, certificates, etc.. The capabilities of these toolkits include nearly everything available in Security Manager Administration (the administrative client), but packaged as a library of APIs instead of as an executable with a graphical user interface.

There are two PKI administration toolkits: The Administration Toolkit for C (for C programmers) and the Administration Toolkit for the Java Platform (for Java programmers).

Classic Toolkit

The Classic Toolkit is useful for developing Secure Identity Management, Secure Messaging, and Secure Data applications. It was originally designed to integrate with Entrust Entelligence Desktop Solutions (EDS), and is still useful for that purpose – to add security capabilities to desktop applications where EDS is resident. But this toolkit is also useful for adding security to standalone applications (without EDS present).

This classic toolkit not only provides security services (e.g., authentication, encryption and digital signature) to your application, but also provides valuable integration services, including: single-login with other Entrust applications, PKI integration, automatic key and certificate life-cycle management.

Note: Some Entrust customers may have deployed Entrust Entelligence Security Provider (ESP) instead of EDS. The classic toolkit was not intended to work with ESP. Since ESP is essentially a cryptographic service provider (CSP) for the

Microsoft Security Framework, the recommended approach for integrating your application with Entrust ESP would be to use the Microsoft CryptoAPI.

- The PKCS#7 Toolkit for C is used by applications which need to encrypt and/or sign data in conformance with the PKCS#7 standard.

This classic toolkit is currently in use by both partners and enterprise customers to add security to your applications, access Entrust credentials, and provide full key and certificate management capabilities.

Other Toolkit Utilities

Sometimes it is desirable to gain programmatic access to basic encryption and digital signature capabilities, but without the need (or resource investment) to develop an application using C or Java APIs. Sometimes it is preferable to simply invoke these capabilities at a higher level from within a script. This approach can significantly reduce your development and support effort. The Entrust Authority Command Line Utility can be used for just this purpose.

This Command Line Utility is an executable which can be invoked from a Windows or Unix command line (or from within a script) using its rich command-line interface. It can be used to perform encryption/decryption of files, and signature creation/verification as well. The development time using this utility would be a mere fraction of the time that would be necessary to build a similar application using C or Java APIs. Command Line Utility can also automatically access and manage the Entrust credentials (epf) as necessary.

Server Login is a utility which complements the Entrust toolkits (and other Entrust applications). It provides automatic (unattended) login to Entrust credentials. This capability is essential for server applications, where a person is not available to type in a password upon startup. Server Login works with all of the toolkits, as well as Command Line Utility.

Licensing

The Entrust toolkits are available to Entrust Technology Partners for development purposes. Term (s) and usage guidelines are outlined in the toolkit shrink wrap licensing agreement.

If you would like to distribute an Entrust toolkit engine with your application, contact your Entrust partner representative at entrust.ready@entrust.com. Partners require an Engine Distribution Agreement and must pay the applicable fees in order to distribute the Entrust toolkit engines.