



Entrust Authority™ Toolkits

Grow your Business, Increase Trust, ROI

The Entrust Authority™ Toolkits are security integration APIs that enable customers and partners to improve service levels and cost-effectively achieve time-to-market goals with easy integration of proven security into critical business applications. Developers can rapidly build and deploy scalable applications with flexible security services using X.509-managed certificates.

The toolkits provide a secure framework where sensitive information remains private. This is essential for B2B, B2C, G2C and enterprise applications and transactions to remain trusted. By implementing a strategy from the security experts, you can deliver new revenue at a lower cost while your developers focus on what they know best — your business.

The Product

Entrust Authority Toolkits are comprised of two main components:

1. A software development kit used by developers to integrate security capabilities such as digital signature or encryption into their applications.
2. Cryptographic engines that are distributed to the server or client application and perform security functions such as digital signatures and encryption of e-mail, files, etc.

Product Features

When the toolkits are used in combination with the Entrust PKI, organizations can automate digital certificate management, centrally define policy and control application behavior to comply with regulatory and organizational requirements.

- FIPS-validated, trusted framework for successful e-business development
- Broad platform support
- High-level APIs that leverage Entrust's cryptographic expertise, minimizing risk of security breaches

Do you require?

- Cost-effective strong security for internal or external applications?
- The ability to rapidly add new services or improve existing service levels using proven security?
- The ability to bundle security with products you sell?
- Secure open standards-based file exchanges with partners, customers and suppliers?
- Data protection to safeguard competitive advantage and comply with government regulations such as Sarbanes Oxley (SOX), California Senate Bill 1386, HIPAA or GLBA?
- The ability to build custom S/MIME applications?
- Consistent security across applications and platforms independent of individual developer/user decisions?



- Option to integrate with Entrust's comprehensive PKI management capabilities
- Security Toolkit for Java enables organizations to integrate security capabilities in applications in a heterogeneous, multivendor environment
- FIPS-validated, trusted framework for successful e-business development

Organizations can leverage hardware and software integration completed with Entrust TrustedPartners (www.entrust.com/partners).

- Administration Toolkit for C: develop customized registration and administration processes for Entrust/PKI
- Security Toolkit for the Java platform: develop interoperable Java applications, applets or servlets
- PKCS#7 Toolkit for C/C++: create S/MIME and Privacy Enhanced Mail (PEM), store and forward applications

Technical Features:

- Strong certificate-based authentication using X.509v3 standard
- Permanent digitally signed records of transactions
- End-to-end protection of data via adding encryption to custom file transfer applications
- Persistent encryption of data at rest on the organization's networks, databases and servers

- Easy interoperability and extensibility through compliance with open standards, XML digital signature and encryption standards
- Non-repudiation through time-stamped S/MIME and PKCS#7 documents
- High-level Application Protocol Interfaces for reduced development time and lower costs
- Broad support for smart cards, tokens, HSMs, policy certificates and client-side settings to enforce corporate guidelines
- Path validation per X.509 and RFC3280 standards as required for the NISTPKI Test Suite

Supported Platforms: Platform coverage varies by toolkit.

Details at: www.entrust.com/authority/toolkits.htm

Pricing and Availability

Organizations looking to build commercial applications on a strong FIPS-validated, trusted framework can cost-effectively add security to the products that they sell. Organizations looking to bundle security with applications they sell should ask about royalty-based pricing.

About Entrust

Entrust [NASDAQ: ENTU] secures digital identities and information for consumers, enterprises and governments in 1,650 organizations spanning 60 countries. Leveraging a layered security approach to address growing risks, Entrust solutions help secure the most common digital identity and information protection pain points in an organization. These include SSL, authentication, fraud detection, shared data protection and e-mail security. For information, call 888-690-2424, e-mail entrust@entrust.com or visit www.entrust.com.

Entrust[®] Securing Digital Identities & Information

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. In Canada, Entrust is a registered trademark of Entrust Limited. All other Entrust product names and service names are trademarks or registered trademarks of Entrust, Inc. or Entrust Limited in certain countries. All other company names, product names and logos are trademarks or registered trademarks of their respective owners. © Copyright 2007 Entrust. All rights reserved.