



Entrust Solutions for the U.S. Department of Defense

Interoperable Security and PKI Solutions

Entrust is a recognized leader in public key infrastructure — commonly known as PKI — and information security solutions among defense and civilian government agencies and private sector organizations. Headquartered in Addison, Texas, Entrust provides interoperable PKI and non-PKI solutions to more than 1,700 customers around the world who have stringent security requirements and complex environments. Entrust technology also serves as the foundation for the vendor-neutral U.S. Federal Bridge Certificate Authority (FBCA), which enables digital certificate interoperability between various domains internal and external to the U.S. Federal government.

And with the Joint Task Force-Global Network Operations (JT-GNO) order requiring the rapid, aggressive deployment of PKI and public key enabling authentication, digital signatures and encryption, Entrust serves as a trusted, valuable partner.

Entrust solutions address a wide variety of security issues. Our versatile authentication platform helps secure and authenticate individuals, devices and applications. Entrust encryption solutions help keep data secure, whether at rest (e.g., on a hard drive or portable media) or in transit (e.g., e-mail). In short, Entrust has industry-leading solutions to help solve many security challenges.

DoD has been at the forefront in implementing PKI and leveraging its benefits, notably with the Common Access Card (CAC). Several Entrust solutions are designed to work with the CAC and have been tested and certified by the Joint Interoperability Test Command (JITC).

Industry-leading Solutions for Public Key Enablement

Entrust Authority PKI manages the full lifecycle of certificate-based digital identities. Optional PKI components can be easily integrated to help satisfy unique security requirements and transparently automate security-related processes through a single PKI. Entrust Authority PKI is FIPS-140-2 validated and meets the Common Criteria (EAL4+) standard.

Entrust Serves:

- 8 of the top 10 e-governments worldwide
- 8 of the top 10 global telecom companies
- 7 of the top 10 global pharmaceutical companies
- 8 of the top 10 global aerospace and defense companies
- 7 of the top 10 global commercial savings banks
- 4 of the top 5 global petroleum companies

Entrust customers have stringent security requirements:

- U.S. State Department
- U.S. Justice Department
- U.S. Federal Bureau of Investigation
- Royal Canadian Mounted Police
- UK Ministry of Defence
- Norwegian Ministry of Defence
- Among many others ...



Entrust Authority Auto-enrollment Server adds the capability to automatically enroll or re-enroll people, processes, devices and non-person entities for managed certificates, simplifying deployment and ongoing operations.

Entrust Authority Roaming Server enables users to authenticate and have secure access to sensitive information from any location.

Entrust Authority Toolkits help developers apply best-in-class, PKI security to custom applications. These specialized FIPS 140-2-compliant toolkits provide a common set of services to permit developers to rapidly deploy applications that solve business problems without having to spend valuable development cycles creating these common services.

Entrust TruePass™ is PKI-agnostic and can be used to effectively PK-enable Web-based applications. Entrust TruePass provides end-to-end Web security and protects information during bidirectional transmission over networks (e.g., browser to server, server to browser) and while stored on Web and back-end servers. This zero-footprint Java applet facilitates deployment and helps enable security for legacy applications with less integration and programming. Entrust TruePass has achieved FIPS 140-2 Level 1 certification. Entrust TruePass version 7.0 is JITC-Certified.

Entrust Managed Services PKI enables organizations to take advantage of PKI without building and maintaining the infrastructure in house. Entrust Managed Services PKI is a service that offers all the benefits of Entrust's industry-leading solutions with a flexible delivery method that allows organizations to buy only what they need. The Entrust Managed Services PKI is also available as a FICC-certified Shared Service Provider.

In addition, Entrust offers a comprehensive range of PKI-related applications, toolkits and services through our wholly owned subsidiary CygnaCom, which has provided professional computer security services and cryptographic solutions to governments and organizations since the inception of PKI technology.

Other Industry-leading Security Products

Entrust Intelligence™ Group Share enables the efficient sharing of network files and folders among work groups while maintaining the security of the data through automatic, transparent and persistent encryption. Entrust Intelligence Group Share is easy to deploy and manage since the client footprint is small and a PKI is not required.

Entrust Intelligence Messaging Server makes it possible to automatically encrypt e-mail before it is transmitted to recipients outside an organization's messaging environment without requiring any additional desktop software or end-user action. The decision to encrypt outbound e-mail to specific addressees is determined by an encryption policy on either the Messaging Server or a separate content scanner.

Entrust GetAccess™ is a scalable Web access control solution that centrally manages access to multiple applications through a single portal, providing users with single sign-on (SSO) to the applications and content they are authorized to see. Currently one of only 10 solutions on the GSA's Approved E-Authentication Technology Providers list, Entrust GetAccess can be deployed as a powerful Federated identity management tool and enables government agencies to reduce administration costs while driving more services through citizen-facing Web portals.

Entrust IdentityGuard, an award-winning versatile authentication platform, provides a range of open multifactor authentication capabilities so organizations can tailor security implementations based on risk or threat assessments. For less sensitive applications not requiring the CAC, Entrust IdentityGuard is an affordable way to upgrade security from passwords for user populations such as citizens or dependents. For more sensitive applications such as personnel and financial applications, Entrust IdentityGuard can provide two-factor authentication when used in conjunction with a CAC card or other public-key-enabled tokens.

About Entrust

Entrust [NASDAQ: ENTU] secures digital identities and information for consumers, enterprises and governments in 1,700 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 2008 Entrust. All rights reserved.