



## Entrust Authority Security Manager

### Manage Your Certification Authority with Ease

Deploying digital certificates allows an organization to leverage encryption and digital signatures to support a variety of security services, including user and device authentication, transaction integrity and data security.

Entrust Authority Security Manager, the world's leading public key infrastructure (PKI), is designed to help organizations easily manage their security infrastructure. This certification authority (CA) system allows organizations to easily manage the digital keys and certificates that are used to secure user and device identities.

### The Product

Deployed at the server-level, Entrust Authority Security Manager software enables valuable security capabilities — including digital signature, digital receipt, encryption and permissions management — to be applied across a wide variety of enterprise applications.

With the automatic and transparent key and certificate management delivered by Entrust Authority Security Manager, users do not need to know anything about security to leverage the enterprise security features.

In addition, Entrust Authority Security Manager provides key backup and recovery of keys and key history so that organizations can have confidence that encrypted information will not get lost if a user loses his or her keys.

With Entrust products, security management is seamless and transparent to the end-user, thereby reducing help desk calls. The solution provides the following capabilities:

- **Securely stores the CA private key**
- **Issues certificates for users and to any device or application supporting the X.509 certificate standard**
- **Publishes certificate revocation lists (CRLs) that are used to verify whether a user or application's certificate is still trusted by the CA that issued it**
- **Maintains an auditable database of users' private key histories for recovery purposes, in the event that users lose their keys**

Leveraging Entrust Authority's optional components, organizations can choose to add further security management capabilities — including automated enrollment, self-registration and self-recovery of digital identities, secure roaming and the use of PINs as an alternative to strong authentication.

### Product Benefits

- **Provides ease of certificate management** — helps manage the digital identities within an organization for company-wide security, without burdening administration
- **Simplifies the user experience** — users do not need to know anything about public keys and certificates to add security to communications and transactions
- **Enables corporate-wide policy management** — helps to enforce security policies relating to passwords, administration and digital certificate settings
- **Offers high levels of interoperability** — includes enhanced integration with Microsoft software to help customers leverage existing investments
- **Available as a hosted service** — leverage the convenience of a full PKI without an expensive upfront investment, in-house experts or need for secure facilities



## Complementary Entrust Products

### Entrust Intelligence Security Provider

This thin-client desktop security software allows organizations to use a single digital identity to add security capabilities beyond authentication to applications such as e-mail or file encryption.

### Entrust TruePass

The Entrust TruePass portfolio provides end-to-end Web security with unmatched ease of use and user transparency. Information that is protected by Entrust TruePass is secure as it is transmitted in both directions over the Internet (browser to server, server to browser) and when it is stored on the Web server and back-end servers.

### Technical Features

- Automated digital ID management including updates, revocation and recovery
- Flexible enrollment options including automated enrollment and self-registration
- Support for unlimited administrators and up to 10 million users per CA
- Web-based administration for delegated and distributed administrative processes
- Centrally managed policies and controls
- Common Criteria EAL 4+ certified
- Comprehensive and customizable auditing and reporting
- Support for peer-to-peer and hierarchical cross-certification of CAs
- Support for certificate standards including X.509 certificate and CRL formats, PKIX-CMP, PKCS#7/10 and SCEP, thus providing interoperability with PKI-aware applications such as virtual private networks, Web browsers, e-mail and e-business applications
- Interoperability with LDAP directories (including Microsoft Active Directory), smart cards, OCSP responders and hardware security modules (including SafeNet and nCipher)

### Platforms Supported

Entrust Authority Security Manager is available for deployment in Microsoft® Windows® and Unix environments.

- Microsoft® Windows® Server 2003 (Postgresql 8.4 database)
- Sun Solaris 10 (IBM Informix 9.4 or Oracle 10G R1/R2 database)
- HP-UX 11i v1 (IBM Informix 9.4 database)
- RedHat Linux 5.4 (Postgresql 8.4 database)

### About Entrust

Entrust provides identity-based security solutions that empower enterprises, consumers, citizens and Web sites in more than 4,000 organizations spanning 60 countries. Entrust's identity-based approach offers the right balance between affordability, expertise and service. For strong authentication, fraud detection, digital certificates, SSL and PKI, call 888-690-2424, e-mail [entrust@entrust.com](mailto:entrust@entrust.com) or visit [www.entrust.com](http://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. © 2010 Entrust. All rights reserved.