

## Entrust Authority Security Manager

### Managing an In-House 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 verification, and data security.

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

### Simplified Certificate Management

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

With 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.

The platform also provides key history, backup and recovery features so organizations have confidence encrypted information will not get lost if users misplace their keys.

### Mobile Security

Mobile operating systems inherently have the ability to store certificate-based credentials and make them available to applications — such as VPN clients and email software — that run on the device. Entrust Authority Security Manager issues certificates to mobile devices, enabling organizations to protect their mobile network.

Entrust Authority Security Manager may generate certificates for mobile devices as requested by Entrust Authority Administration Services or the Entrust IdentityGuard software authentication platform. And both solutions provide a common Web service interface for enrolling and managing certificates issued to mobile devices.

### Product Benefits

- Manages the digital identities within an organization for company-wide security, without burdening administration
- Simplifies the user experience; users do not need to understand public keys and certificates to add security to communications, mobile devices and transactions
- Helps enforce corporate-wide security policies relating to passwords, administration and digital certificate settings
- Offers high levels of interoperability, including enhanced integration with Microsoft software to help customers leverage existing investments
- Allows organizations to identify, manage and authenticate mobile devices used on the corporate network

## SOLUTION CAPABILITIES

With Entrust PKI products and services, security management is seamless and transparent to the end-user, thereby reducing help-desk calls.

### Secure Storage

Entrust securely stores the CA private key to ensure the integrity of your in-house CA infrastructure. The solution also maintains an auditable database of users' private key histories for recovery purposes.

### Easy Certificate Issuance

Issue certificates for users, applications or devices, including tablets and smartphones, that support the X.509 certificate standard.

### CRL Control

Publish 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.

### End-User Convenience

Leverage an advanced security infrastructure that accommodates users who log in from different workstations, work offline or from mobile devices, or use various methods of authentication (e.g., smartcards, tokens or biometric devices).

### Perfected Automation

Take advantage of the solution's automated key and certificate lifecycle management capabilities. Users do not need to know anything about public keys and certificates to add security to communications, devices or transactions.

### Optional Enhancements

Leveraging Entrust Authority Security Manager's optional components, organizations can choose to add further security management capabilities — including automated enrollment, self-registration and self-recovery of digital identities and secure roaming.

---

## EPASSPORT FOUNDATION

Entrust Authority Security Manager is a mandatory component of an Entrust ePassport system. The solution may be configured as a Country Signing Certification Authority (CSCA), Country Verifying Certification Authority (CVCA) or a Document Verifier (DV) to issue certificates used to secure ePassports. Entrust also offers a variety of complementary components that help streamline any ePassport ecosystem.

---

## 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 email 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.

### Entrust Authority Administration Services

This component provides Web-based applications and services that interact with Entrust Authority Security Manager to manage digital IDs and certificates. Services include administration interfaces that allow administrators to manage users and certificates, and enrollment services that allow users and non-human entities (e.g., computers and mobile devices) to enroll for certificates. Entrust Authority Administration Services also enables auto-enrollment of users and machines.

### Entrust Authority Roaming Server

Roaming Server adds mobility to the enhanced security capabilities of the Security Manager system. The server provides users with secure access to digital content from any location without the need for users to carry the digital IDs required to establish secure connections.



### **Entrust Authority Security Manager Proxy**

Security Manager Proxy allows the operation of Security Manager over the Internet using standard Internet protocols without making changes to existing firewall settings.

### **Entrust Authority Toolkits**

Entrust Authority toolkits provide a common set of services that permit developers to deploy applications that solve business problems without having to spend valuable development cycles creating these common services.

### **Entrust Entelligence Group Share**

Entrust Entelligence Group Share is a client-server application that allows users to secure the contents of selected folders on corporate networks.

### **Entrust Entelligence Messaging Server**

This appliance-based email security solution delivers comprehensive, standards-based email encryption capabilities, simplifying secure communication with external business partners and customers.

### **Entrust GetAccess**

This scalable Web access management solution provides authorization and sign-on capabilities to Web applications. Entrust GetAccess employs dynamic, context-sensitive policies to control user access to company resources.

---

## **TECHNICAL FEATURES**

- Automated digital ID management including updates, revocation and recovery
- Support for unlimited administrators and up to 10 million users per CA
- Web-based administration for delegated and distributed administrative processes available via optional Administration Services component
- Centrally managed policies and controls
- Certified for Federal Information Processing Standards (FIPS) 140-2 Level 2
- Common Criteria EAL 4+ certified
- Comprehensive and customizable auditing and reporting
- Support for peer-to-peer and hierarchical cross-certification of CAs
- Support for standards including X.509 certificates and CRL formats, PKIX-CMP, PKCS#7/10 and SCEP (via Entrust Enrollment Products); provides interoperability with PKI-aware applications such as virtual private networks, Web browsers, VPN devices, mobile devices, email and business applications
- Interoperability with LDAP directories (including Microsoft Active Directory), smartcards, OCSP responders and hardware security modules (including SafeNet and Thales)

---

## **PLATFORMS SUPPORTED**

Entrust Authority Security Manager is available for deployment in Microsoft® Windows®, UNIX and Linux environments.

- Microsoft® Windows® Server 2008 R2 (Entrust PostgreSQL 8.3.11 database)
- Oracle® Solaris 10 (Entrust PostgreSQL 8.3.11, Oracle Database 10G R1/R2 or Oracle Database 11G R1/R2 database)
- HP-UX 11.31 (Entrust PostgreSQL 9.0.7)
- Red Hat Enterprise Linux 5.4 or later versions of 5.x (Entrust PostgreSQL 8.3.11 database)
- Red Hat Enterprise Linux (6.0-6.2)



**SECURITY  
ON**

## Entrust & You

More than ever, Entrust understands your organization's security pain points. Whether it's the protection of information, securing online customers, regulatory compliance or large-scale government projects, Entrust provides identity-based security solutions that are not only proven in real-world environments, but cost-effective in today's uncertain economic climate.

Entrust's identity-based solutions empower enterprises, consumers, citizens and websites in more than 5,000 organizations spanning 85 countries. This 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**, email **entrust@entrust.com** or visit **entrust.com/pki**.

## Company Facts

Website: [www.entrust.com](http://www.entrust.com)  
Employees: 359  
Customers: 5,000  
Offices: 10 globally

## Headquarters

Three Lincoln Centre  
5430 LBJ Freeway, Suite 1250  
Dallas, TX 75240 USA

## Sales

North America: 1-888-690-2424  
EMEA: +44 (0) 118 953 3000  
Email: [entrust@entrust.com](mailto:entrust@entrust.com)

## About Entrust

A trusted provider of identity-based security solutions, Entrust secures governments, enterprises and financial institutions in more than 5,000 organizations spanning 85 countries. Entrust's award-winning software authentication platforms manage today's most secure identity credentials, addressing customer pain points for cloud and mobile security, physical and logical access, citizen eID initiatives, certificate management and SSL. For more information about Entrust products and services, call **888-690-2424**, email **entrust@entrust.com** or visit **www.entrust.com**.

**Entrust**<sup>®</sup> Securing Digital Identities & Information