Entrust®
Securing Digital Identities & Information

Government-Strength Security For Your Organization

Protecting Your Desktop Applications With Enhanced Security Solutions

Summary

This white paper addresses the key drivers for securing enterprise desktop applications and presents the benefits of deploying enhanced security solutions that offer your organization 'government-strength' security—security that is developed to meet government requirements for electronic data privacy, integrity of content and origin for audit trails and compliance with industry regulations.

April 2004

The material provided in this document is for information purposes only. It is not intended to be advice. You shall be solely responsible for acting or abstaining from acting based upon the information in this document. ENTRUST DOES NOT WARRANT THE QUALITY, ACCURACY OR COMPLETENESS OF THE INFORMATION CONTAINED IN THIS DOCUMENT. THIS INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATIONS, WARRANTIES, AND/OR CONDITIONS OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, WARRANTIES AND/OR CONDITIONS OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT, TITLE AND FITNESS FOR A SPECIFIC PURPOSE.

Entrust®
Securing Digital Identities & Information

Table of Contents

1 Introduction

All types of enterprises, organizations and governments rely on computer workstations (desktops and laptops), to operate efficiently in today's economy. Communications, negotiations, research and transactions are all conducted via electronic file creation and transit over a corporate intranet, private network or the Internet. The cost savings, shorter time to market and wider organizational reach made possible by the use of enterprise workstations are compelling benefits that have driven the exponential growth of the desktop market.

Most organizations have numerous file and application servers dispersed throughout the corporate network, in addition to at least one workstation for every employee. The workstation is critical in that it provides a single access point to all corporate information and resources (directories, servers, applications). Contained within these resources is a wealth of information, including that of a sensitive nature, such as R&D results, strategic plans, sales forecasts, financial statements, human resource records and customer lists. *But how secure are these files?*

The very mobile nature of the electronic mediums that the sensitive information is stored on puts an organization at higher risk for unauthorized access (hacking) and theft. With globally dispersed work teams, traveling sales people and interested third parties such as business partners and suppliers, organizations are at a greater risk of laptop theft and loss of sensitive data. The implications of information theft are serious, including lost revenue, regulatory penalties and the potentially devastating loss of brand reputation and goodwill. For example, if the latest drug delivery methods and patent pending information are stolen from a pharmaceutical company and placed into the hands of competitors, the company could lose its edge in penetrating the market first.

In order to realize the full potential and take advantage of the flexibility, mobility and collaborative opportunities that desktops and laptops afford, organizations need to be able to provide confidentiality of documents and strong authentication of the individuals with authorization to view them. This is precisely why more and more organizations, including government departments and financial institutions that conduct business electronically, are implementing stronger security for the files and folders that reside on their organizations' electronic devices and for the enterprise applications such as messaging and electronic forms that are used across their organizations.

This paper addresses the need for securing enterprise data and applications and the value of deploying ***'government-strength'*** security solutions within your organization. It also provides an overview of how Entrust® security solutions can help you meet this challenge.

2 The Need for Desktop Protection

The very openness that has stimulated the adoption and growth of private networks and the Internet also threatens the privacy of individuals, the confidentiality of data, and the accountability and integrity of business transactions. Key concerns include risk of theft, alteration, interception and dissemination of confidential data, as well as fraud, damage to reputation and economic loss. The risk of data theft can be quantified through industry research. According to the **DTI Information Security Breaches Survey 2004**, confidentiality breaches tend to cause major disruption to organizations over a long period of time (longer than a month in 15% of cases). The report said, "Remediation and investigation involved significant staff time (10-20 person days, on average). These breaches also resulted in the largest direct cash expenditure of any security incidents." Threats to information security arise from external sources such as competitors and computer hackers, as well as internal sources, such as disgruntled employees and contractors. A further challenge for organizations is protecting information for both regulatory compliance and the prevention of cyber-terrorism. The following are some of the key concerns organizations face today that drive them to deploy security solutions for their enterprise desktop infrastructures.

Regulatory Compliance

Increased awareness of transaction auditing has resulted in the development of several new items of government legislation that require governments and enterprises to provide enhanced security and audit of sensitive information and transactions. Examples of such regulations include **Sarbanes-Oxley** for financial reporting controls, **HIPAA** for healthcare providers, which require that they protect electronic health information, and **Gramm-Leach-Bliley** that requires financial institutions to develop and implement appropriate safeguards—including a written information security plan—to protect customer information. Other regulations such as **California SB 1386** require that companies and government agencies notify customers if their unencrypted personal information has been acquired by an unauthorized entity.

Mobility of the Workforce

With global staff and traveling employees, an organization's most valuable asset—intellectual property—is at risk of theft and viewing by unauthorized individuals. Preventing laptop theft is one thing, but protecting the sensitive data stored within a laptop in the event that it is stolen, is of utmost importance.

Controlled Access to Sensitive Information

Almost every enterprise and government agency has a significant need to allow only authorized individuals to have access to sensitive information. Setting parameters for the files and folders and applications that users are allowed to view and utilize is crucial to protecting the integrity of an organization's data.

Work Group Collaboration

The proliferation of virtual teams means employees have a greater need to share information over internal networks and work together in building strategy and executing deliverables. As such, it is important to protect access to sensitive shared documents while limiting the rights to view, create and edit content, to only authorized individuals.

> *"Companies that fail to address the security issues that affect distributed computing environments will see the cost of desktop security-incident management rise by 30 percent or more annually, as the number of attacks continue to increase through at least 2005. A single security breach related to regulation or legislation can put companies at significant risk of a significant financial loss or public relations disaster."*
>
> **Source:** "Best Practices: Desktop Security," David Friedlander and Jan Sundgren, **Forrester Research**, January 30, 2004.

3 What is 'Government-Strength' Security?

Entrust defines 'government-strength' security as a level of data protection commensurate with that adopted by government agencies who have a responsibility for ensuring a high level of information security. Government-strength security must meet stringent requirements set out by government authorities and comply with information security standards and regulations for non-classified material. The following sections describe key security criteria and address one of the main governing bodies for security, and one of its test suites.

Government-Strength Security Criteria

When considering what contributes to a government-strength security solution, there are several key criteria that should be enabled by the solution. These criteria include a range of technical features, capabilities, and processes, as outlined below.

Common Layer of Security
The solution should enable the application of a common layer of security across the enterprise application infrastructure that provides consistent security at all times, independent of the particular application that may be in use.

Consistent Application of Policy
The solution should allow the application of security policy in a consistent way across the organization, while allowing flexibility to accommodate the needs of unique applications.

Government-Recommended Use of Cryptographic Algorithms
The solution should support a wide selection of industry-leading cryptographic algorithms that utilize the latest developments in longer cryptographic key-lengths. Current algorithms include:

- SHA-1, SHA-256
- DES, Triple DES, AES
- Elliptic Curve Cryptography (ECC)
- DSA
- RSA

Management of User Roles and Application of Policy on a Per-User Basis
The solution should provide a way to easily manage user roles and access privileges for unique applications while enabling the application of security policy according to the rights and responsibilities of individual users.

Flexible Levels of Strong Authentication
The solution should offer flexibility to enable the level of authentication required by the organization, for specific sets of users and within specific applications. It should also support the use of strong two-factor authentication by offering storage of digital IDs on tokens or smart cards.

Government-Approved Security Level
The solution should be designed to achieve the highest security levels that can withstand external security evaluations (such as FIPS 140-2) that show it is resistant to attack. As such, the solution should provide protection for all keys used and operations performed.

Path Validation

Path validation is the set of processes applied to a certification path that checks whether a certificate is trustworthy and appropriate for the intended use. Each certificate in the path may include a set of constraints that limit the bounds of the federated trust established through the path. Additional constraints may be supplied as an input to the process itself (e.g. one certificate user may require that trust be based on a “high assurance” policy while another may only require “medium assurance”). Path validation performs tests on the certificates in the path to determine whether the certificates are valid, a proper chain of trust is established, and all constraints have been adhered to. The process is a critical element of protecting the interests of certificate users so that they only use certificates in accordance with their local security policy.

NIST PKITS Test Suite

Path validation is a relatively complex process and until recently there has not been a comprehensive test suite available to assess conformance. Any implementation could ‘claim’ to perform path validation but there was no independent way to assess the correctness of those implementations. In 2003, the **National Institute of Standards and Technology (NIST)**, together with the National Security Agency (NSA) and DigitalNet, produced a complete test suite that tests path validation implementations to determine whether they perform elements of path validation in conformance with the standard definitions in X.509 and RFC 3280. The test suite, known as Public Key Interoperability Test Suite (PKITS) provides test descriptions as well as test data for all aspects of certification path validation.
The complete suite is available at: http://csrc.nist.gov/pki/testing/x509paths.html

Path Validation Profiles

Path validation is a complex process that includes many optional features and PKITS tests these. It is not expected that all implementations will support every possible option, nor is it expected that all optional features will be necessary in all environments. NIST has drafted a set of “profiles” that group the optional features into functional packages. One of these packages can be provided for path validation implementations aimed at claiming conformance to a “bridge-enabled” profile. That profile describes the necessary functions and identifies the specific PKITS tests that must be passed in order to claim conformance to the bridge type of trust environment deployed by several governments for multi-agency applications. An initial draft of the **NIST Recommendation for X.509 Path Validation** was published in April, 2004 and is available on the NIST web site at: http://csrc.nist.gov/pki/testing/NIST_Recommendation_for_X509_PVMs.pdf

This document specifies functional requirements for path validation modules (PVMs). The requirements are broken up into two major categories: Enterprise PVMs for use in PKIs that are limited to a single organization and Bridge-enabled PVMs for use in multi-organizational PKIs. The document also includes support for specifying supplementary requirements such as the ability to process delta-CRLs or indirect CRLs. An appendix is included that indicates how PKITS can be used to verify that a PVM implements path validation correctly.

The bridge-enabled profile identifies the necessary components and tests for path validation for meeting Entrust-defined ‘government-strength’ security.

4 Why is 'Government-Strength' Security Important for Your Organization?

Given the requirements in today's business world to comply with increasing regulations, enterprises need to deploy a high level of security that meets their needs and falls within their allowable budgets—all while utilizing security that is easy for the organization to deploy and manage and easy for end users to adopt. Many government agencies demand stringent security requirements and are already benefiting from deploying enhanced security solutions. Enterprises can leverage these benefits for enhanced security across their desktop application infrastructures for increased efficiency, protection of information and compliance with specific industry regulations pertaining to the protection of data privacy.

To Comply With Regulations

There may be specific legislation that governs your business processes, and the government is typically the driving force behind such legislation. The fact that government agencies dictate specific requirements related to security software and implement those requirements within their day-to-day business practices means that they deem the level of security as sufficient, and therefore can provide an organization with confidence that its security is on par with that of governing bodies.

To Adhere to Levels of Security Benchmarked by Government

Internally, Governments set various requirements for tight security and assign governing bodies (such as NIST) with responsibilities for developing security standards that they can align with when identifying and deploying the most up-to-date technology available. One such example is NIST's creation of the PKITS test suite that recommends specific testing and guidelines that agencies should follow when implementing security solutions.

To Help Implement Information Security Governance

Information Security Governance is top-of-mind for organizations around the globe today. Defined, Information Security Governance (ISG) is a subset of Corporate Governance dealing with the policies and internal controls related to information resources and their security. Corporate scandals, coupled with increasing legislation have prompted shareholders to demand better accountability from public firms. By deploying government-strength security solutions, organizations become proactive in aligning their corporate practices with the proven best practices of government agencies that are concerned about utilizing a high level of security.

5 The Requirements for Effective Enterprise Desktop Security

The benefits of workstations and mobile devices are compelling, but several challenges exist that need to be addressed before organizations are able to realize greater efficiencies and reduce the risk of information theft. Despite large investments in perimeter security like firewalls and intrusion detection, the volume of security breaches continues to grow at an alarming rate. According to the **2003 US CSI/FBI Computer Crime and Security Survey**, 56% of respondents reported unauthorized use, and theft of proprietary information caused the greatest financial impact, with an average loss of $2.7 million.

No longer are hackers striking exclusively from online. Computer hard-drives and other pieces of hardware containing critical information have, and will continue to be, stolen. Moreover, employee workgroup collaboration results in larger numbers of users accessing the same file repositories and organizations are challenged to maintain the integrity of content. Even information that can only be accessed via an office workstation requires security, because people internal to an organization undertake the majority of security breaches. As a result, it is imperative to protect the actual data at its source—the desktop.

> *"Provide consistent policies, authentication mechanisms, and security services across all connections, regardless of user location. Security must become an embedded way of life for the members of the mobile community. By removing the choices of security or authentication processes from the user, the network manager can be assured that the appropriate protection mechanisms are in place."*
>
> **Source:** "Managing and Securing the Mobile Device," Michael Disabato, **Burton Group**, April 5, 2004.

To facilitate widespread use of desktop security while reducing the impact on IT resources, a data protection solution must be easy to deploy, use and manage. Moreover, it must fit within the corporate IT budget. In building a business case for a data protection solution, there are six primary requirements to take into consideration. A well-designed solution must:

1. Deploy rapidly and easily
2. Reduce impact on current IT applications, business processes, administrators and end users
3. Provide flexible access control and the ability to limit viewing rights for specific files or folders
4. Mandate strong, easy to use security for highly sensitive files and folders
5. Drive lower total cost of ownership through the provision of automatic and transparent user identity management
6. Extend easily to secure additional applications (e-mail, VPN, WLAN, e-forms, etc.)

6 Deploying Entrust Security Solutions for 'Government-Strength' Security

Entrust security solutions make it possible for organizations to leverage the benefits of identity and access management to move more processes and applications online. By protecting information privacy and helping to provide secure access to customers, partners and employees, Entrust® solutions can help organizations extend their services while improving compliance with regulatory demands for stronger internal controls and information privacy. Entrust security solutions are designed to overcome a common problem in most security implementations—human nature. When individuals need to understand security or jump through hoops in order to use it, they may use it incorrectly or not at all. Through tight integration with desktop applications, Entrust security automation and functionality is virtually transparent to end users. Furthermore, Entrust solutions are designed to meet the latest security requirements of major governments and industry regulations—thereby offering organizations **'government-strength'** security.

Entrust Entelligence™ Desktop Security Products

The Entrust Entelligence™ Suite of Desktop Security Products provides a key underlying security framework for all of Entrust's core security solutions: Secure Data, Secure Messaging and Secure Identity Management. Focused on securing desktop data wherever it may be contained (within files and folders, e-mail, electronic forms or other applications) and securing the exchange of that data with employees, customers and partners, Entrust desktop security products offer organizations enhanced security. The products help to create a secure workstation environment for employees by enabling the following:

A single secure access point to an organization's information and resources
By securing digital identities and enabling secure authentication of users, Entrust Entelligence Desktop Security Products protect access to the workstation, which is often the user's single gateway to an organization's sensitive information and resources.

Protection of sensitive information from unauthorized viewing
Through encryption of files and folders, the Entrust Entelligence Desktop Security Products provide privacy of information by allowing only authorized users to decrypt protected files for viewing of sensitive content.

NIST PKITS Validation

The Entrust Entelligence Suite of Desktop Security Products has been tested against the **National Institute of Standards and Technology's Public Key Interoperability Test Suite (NIST PKITS)**. This security test suite provides a comprehensive set of conformance tests. Product compliance with NIST PKITS delivers increased risk mitigation for governments and enterprises by testing the set of processes, technically known as 'certificate path validation,' that are executed by users or applications that rely on digital identities. These processes check whether the identity a user or application is planning to use is ***authentic***, ***issued by a trusted authority***, ***valid*** and ***appropriate for the intended use***.

The Entrust Entelligence Suite of Desktop Security Products Version 7.0 has passed all PKITS tests relevant to its path validation functionality, including the following:

- Processing of all certificate extensions used to enforce constraints on policy, naming and path length.

- Capability to initialize all relevant path validation variables on a per-user/group basis. This enables path validation to be performed under different initial conditions by different users depending upon their specific needs. For example, some users may require a "high assurance" policy while others can validate for their applications under a "medium assurance" policy.

- All checks on certificates to determine whether the certificates have valid syntax, integrity, proper key usage settings, have not been revoked, contain no unrecognized critical extensions and are within their validity periods.

- All checks on certification path structure to determine whether the names and keys in adjacent certificates chain properly, the path does not include duplicate certificates, and all intermediate entities represented in the path are Certificate Authorities (CAs).

Entrust Entelligence™ Desktop Manager

Entrust Entelligence™ Desktop Manager is the primary component of Entrust's flagship suite of desktop security products that provide authentication, authorization, digital signatures and encryption for securing enterprise data and applications. A client-based desktop security platform designed to help meet government security standards, Entrust Entelligence Desktop Manager is used extensively throughout government agencies and departments globally and is being adopted by enterprises wishing to extend added security across their business practices. A key component of Entrust's solutions for Secure Data, Secure Messaging and Secure Identity Management, the product provides a single security layer that can be used consistently across a wide variety of enterprise applications to provide authentication, authorization, digital signatures and encryption. It also can provide complete lifecycle management of users' digital IDs that are needed for securing applications—a key benefit that can result in faster deployment and easier administration of users' security credentials.

Secure Data

As the barrage of information security intrusions and losses has escalated, so too have the number of information security reports, laws and regulations. Increasingly, organizations are recognizing information security as a requirement for sound corporate governance—not one that is solely the responsibility of the CIO (or CISO), nor a problem that technology alone can address—but one that requires the active involvement of executive management and employees at all levels in the organization. Entrust's Secure Data Solution provides comprehensive, highly-scalable applications that can help enable organizations to protect information from disclosure, loss or corruption and meet many of the requirements of sound corporate governance. These applications include methods for encrypting data at rest and in transit to secure it in a means commensurate with the risk of its disclosure, loss or corruption without unduly burdening the people and processes that make use of that data.

Security for Files and Folders

Today's workforce uses desktop computers and laptops to write, negotiate, sell, plan, and strategize about the entire future of an organization. These common devices and the networks behind them, have in essence become home to the most important assets an organization has: its intellectual property, sales forecasts, customer or citizen information, strategic plans and other information that the competition or media would like to have. This is precisely why more and more organizations are recognizing the need to secure files and folders that reside on their organizations' electronic devices.

The Entrust® Secure Data Solution enables organizations to turn computer hard drives and networks into secure information storage mediums. Entrust's file and folder encryption products can secure sensitive and valuable information stored on computers, mobile devices and corporate networks. This makes it possible to easily encrypt documents that contain sensitive corporate information. With file and folder encryption, organizations can:

- Store information in an encrypted fashion until it is needed again
- Encrypt documents for a select group of individuals who are authorized to view the contents
- Digitally sign documents online—and, in many jurisdictions, electronic signatures carry the same force of law as those that are handwritten
- Delete documents of a secure nature with confidence that temporary copies that may have been cached will be eliminated as well
- Set certain documents or folders to automatically encrypt, relieving the user or administrator from the responsibility of remembering this task

Mandates strong, easy to use security for highly sensitive files and folders
The Entrust Secure Data Solution mandates strong protection of sensitive information by securing and automatically managing the digital IDs and keys used for encryption of files and folders. Through strong protection of digital identities and strong enforcement of password policies, the solution allows only individuals with the authorized private keys to decrypt protected documents. Working behind the scenes to automatically and transparently manage the digital identities used for encryption of files and folders, the solution frees employees from the responsibility of managing their security profiles.

Provides flexible access control and the ability to limit viewing rights for specific folders or documents

The Entrust Secure Data Solution provides the ability to control access to workstations and limits viewing rights for specific files or folders so that only authorized individuals can access sensitive information. The solution delivers key and certificate lifetime settings and flexible storage options for digital identities. Should the digital identity be stored in the Entrust Security Store, the solution can enforce strong password rules to support an organization's security policy. Offering multiple storage options, the Entrust Secure Data Solution enables the storage of keys and certificates on a smart card, providing the added security of second factor authentication, so that only individuals with the smart card and appropriate access rights are permitted to access the workstation.

Security for E-Forms

E-forms can provide organizations with significant opportunities to reduce costs and improve productivity by moving high-value processes online. Business transformation benefits through the use of e-forms range from significant reductions in business processing time (including reductions in data entry errors) to significant reductions in the costs associated with paper forms. However, to realize the cost-savings and productivity promises of e-forms, organizations need the equivalent of paper-based signatures—they need digital signatures. Digital signatures provide unique capabilities for securing digital information; for example, they can enable the recipient to verify the authenticity of the information's originator. In addition, a verified digital signature assures the recipient that the information has not been tampered with since it was originally signed. In addition to digital signatures, some types of information included in e-forms documents are either private or confidential. The Entrust Entelligence™ Verification Plug-in for Adobe enables the application of digital signatures to Adobe PDF documents and forms. Through

Entrust's encryption capabilities, users of secure electronic forms can easily protect the privacy of sensitive information so that it is only accessible to authorized individuals.

To learn more about how the **Entrust Secure Data Solution** can help add government-strength security to your organization, visit http://www.entrust.com/data.

Secure Identity Management

Your technology environment is likely a large mix of applications, platforms and data types and no two users have the same identity, rights and responsibilities. The responsibility for deploying and managing identities on these systems is spread across your company, challenging you to keep identity data consistent. You need to know who has access to what, how they are using it and what you can do to make their access deeper and better for your business.

The Entrust Secure Identity Management Solution can increase security, improve productivity and help lower the cost of your operations. The solution consists of a comprehensive suite of market-leading identity and access management products that can help organizations easily and securely manage identities and access to information for users, applications and devices, while helping to decrease costs. The key capabilities offered by the Entrust Secure Identity Management Solution that secure desktop environments include strong authentication, authorization and single sign-on.

Strong Authentication

Authentication using digital identities provides a much stronger form of authentication than username/password, allowing organizations to achieve more effective internal controls. Through its Entrust Entelligence™ Desktop Security Products, Entrust offers authentication to a variety of desktop applications. The products also make it possible to deploy strong two-factor authentication to desktops, VPNs, WLANs and Web Portals using SmartCards and USB Tokens.

Authorization and Single-Sign-On

Authorization and single sign-on capabilities address the need for a simplified user log-in experience on the desktop that ultimately can help reduce help desk costs and enhance the security of password management. Entrust capabilities enable organizations to rapidly deploy secure single sign-on to the desktop for all applications for which a user is authorized.

Security for VPNs and WLANs

VPNs and WLANs provide remote workers and offices with anytime, anywhere access to the corporate network at dramatic cost-savings versus over dial-up access or leased lines from telecommunications carriers. VPNs allow an organization to easily build, manage and operate low-cost private networks using the Internet to more efficiently connect mobile and remote workers, remote offices and branch offices more efficiently. Since VPNs and WLANs provide a virtual 'door' from the Internet into the corporate network and all its resources, security is of the utmost importance. The security of a network is only as strong as the method used to identify the users or devices at each end of the communication. By delivering and managing digital IDs for strong identification of users and devices that communicate and exchange information over a VPN or WLAN, Entrust delivers strong security for organizations deploying VPN or WLAN.

To learn more about how the **Entrust® Secure Identity Management Solution** can help add government-strength security to your organization, visit http://www.entrust.com/solutions/identity_management.

Secure Messaging

E-mail is perhaps one of the most important productivity tools in widespread use today. The main purpose of e-mail in business and government is to share information to drive efficient and effective decision-making. But, are you able to fully leverage e-mail to drive productivity or are you hampered by the fact that some of the information you want to share is too sensitive to send over a network? Are you concerned about the privacy of sensitive information stored on e-mail servers and user's disks? And, are you limited in your ability to make decisions and act on e-mail information because you cannot be confident that the sender is who you think it is?

Security for e-Mail Applications

Desktop applications such as e-mail, when used by employees, can increase productivity, streamline business processes and reduce costs. Entrust products enable organizations to encrypt and digitally sign e-mail messages and attachments across a variety of e-mail packages, including Microsoft Outlook and Lotus Notes or Web mail services such as Yahoo! or Hotmail, and even extends security to BlackBerry® wireless handhelds. The Entrust Secure Messaging Solution makes end-to-end secure e-mail easy to use and easy to administer. The solution enables users to send confidential and private information safely over the Internet and protects message contents when stored on e-mail servers and user disks. In addition, through the use of digital signatures, recipients of a message can be more confident in the authenticity and integrity of the communication.

Security for Wireless Messaging

With the proliferation of wireless devices such as PDAs and more advanced mobile phones, wireless messaging has become a key capability for increasing employee productivity. However, to enable this productivity requires that users can feel confident sending sensitive information over the wireless environment. Security is pertinent. To address this issue, Entrust has worked with third-party companies to investigate opportunities for adding security to wireless technologies.

Research In Motion (RIM), a world leader in mobile communications, has extended the capability of its Java™-enabled BlackBerry® handhelds to support S/MIME (Secure Multipurpose Internet Mail Extensions) messaging. RIM's integration with the Entrust Secure Messaging Solution can enable customers to access their secure e-mail from both their BlackBerry handhelds and their desktop PCs using the same digital ID, simplifying both usability and administration.

To learn more about how the **Entrust Secure Messaging Solution** can help add government-strength security to your organization, visit http://www.entrust.com/solutions/messaging.

Competitive Advantages of Entrust Solutions

Benefits of deploying Entrust's government-strength security solutions include:

Risk Mitigation
Enables verification of origin and integrity of document content and can provide confidentiality through encryption and digital signature. Can help mitigate organizational exposure to loss of intellectual property or misuse of sensitive information.

Extension of Products and Services
Helps governments and enterprises to provide high-value products and services online, contributing to improved services for stakeholders and reduced costs.

Ease of Deployment, Use and Administration
Allows users to easily encrypt and sign files without changing their behavior, permitting them to consistently utilize security capabilities within their desktop applications. Use of a single security password can result in easier deployment and administration.

Help in Compliance with Legislation
Helps organizations meet their corporate governance objectives and information protection requirements set out by regulations such as Sarbanes-Oxley, Gramm-Leach Bliley, HIPAA, etc. Can help avoid costs associated with loss of proprietary information by securing access to employee workstations and providing confidentiality of sensitive information stored within the organization's files and folders.

High Return on Investment
Helps extend the security investment by allowing an organization to grow over time to meet changing security policies and align with the overall strategic direction of the company. To start, one enterprise application can be secured, and other applications rolled out subsequently with ease.

7 Protecting Your Enterprise Desktop Infrastructure: The Need to Act Now

Trends in encouraging employee mobility and the increasing globalization of business operations have lead to increased threats of identity and computer theft. In addition, pressure from regulatory bodies for organizations to provide full accountability for online transactions and sensitive information are forcing enterprises and governments to take a direct approach to securing their intellectual property. An enterprise-wide, 'government-strength' data protection solution is not only protection against the potentially devastating loss of proprietary information or non-compliance with regulations, but also a means for helping to drive greater efficiency within an organization.

Entrust desktop security products offer workstation security that is easy for administrators to deploy and manage, and easy for employees to use. Through automatic encryption of files and folders and automated management of digital identities, employees do not need to worry about changing their work behavior for their files and folders to be encrypted for protection from unauthorized viewing or their digital security profiles to be updated. The solution offers smart card storage of user digital IDs for enhanced two-factor authentication so that only those individuals with the smart card, password and appropriate access rights are granted access to the workstation and its secure files and resources. Entrust Security Solutions are unique in that they allow a single user digital identity to be extended to secure a wide variety of enterprise desktop applications including e-mail, file transfer, VPN/WLAN and electronic forms. This allows for rapid deployment of enterprise-wide desktop security and can help contribute to a higher return on investment.

The longer an organization waits to adopt an enterprise data security solution, the greater the risks of compromising sensitive information, risking non-compliance, delivering poor service to users and wasting scarce IT budget and staff resources. This need not be the case, as Entrust security solutions deliver comprehensive capabilities for secure, cost-effective access control for workstations and protection of sensitive information. The solutions are designed specifically for fast enterprise-wide deployments to enable organizations to quickly secure their sensitive resources while lowering administrative costs and increasing services for end users—all factors that help to drive a higher return on investment.

8 About Entrust

Entrust, Inc. [Nasdaq: ENTU] is a world-leading provider of Identity and Access Management solutions. Entrust software enables enterprises and governments to extend their business reach to customers, partners and employees. Entrust's solutions for secure identity management, secure messaging and secure data increase productivity and improve extended relationships by transforming the way transactions are done online. Over 1,250 organizations in more than 50 countries use Entrust's proven software and services to turn business and security challenges into secure business opportunities. For more information, please visit: http://www.entrust.com.