

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



**Securing Your  
Digital Life**

**How Securing Digital Identities & Information Can Help  
Transform Your Business**

*Making the Most Out of Internet & Enterprise Networks*

February 2005

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

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.



## Table of Contents

<b>1</b>	<b>Introduction .....</b>	<b>2</b>
<b>2</b>	<b>Extending the Enterprise, Securely .....</b>	<b>3</b>
2.1	Business Requirements: Identity and Access Management .....	4
2.2	Traditional Approaches to Security Fall Short .....	5
2.3	Securing Digital Identities and Information .....	5
2.4	Identity & Security Management.....	6
<b>3</b>	<b>Making the Most of Internet &amp; Enterprise Networks .....</b>	<b>8</b>
3.1	Secure Messaging .....	9
3.1.1	<i>Secure E-Mail .....</i>	<i>9</i>
3.2	Secure Data .....	10
3.2.1	<i>Secure E-Forms.....</i>	<i>10</i>
3.2.2	<i>Secure Files and Folders.....</i>	<i>11</i>
3.3	Secure Identity Management.....	12
3.4	Security for Web Portals and Web Services.....	12
3.5	Entrust Secure Identity Management Solution .....	13
3.5.1	<i>Strong Authentication .....</i>	<i>13</i>
3.5.2	<i>Authorization and Single-Sign-On (SSO) .....</i>	<i>14</i>
3.5.3	<i>Identity Provisioning.....</i>	<i>15</i>
<b>4</b>	<b>Consistent Security Across an Extended Enterprise.....</b>	<b>16</b>
<b>5</b>	<b>Customers Experiencing a Transformation .....</b>	<b>17</b>
<b>6</b>	<b>About Entrust .....</b>	<b>18</b>

# 1 Introduction

The IT landscape of traditional business is expanding. Business stakeholders are applying increasing pressure to extend the enterprise out to allow greater access to services, systems and information. Built on the foundation of existing relationships and technologies, **extended enterprises** find new ways to create synergies and increase opportunities to positively impact the effectiveness and bottom line of business stakeholders.

Simply put, business is about making decisions. Tighter integration, closer relationships and more open communication enable better decision making. The faster and more accurate the decisions, the better a business can perform. Extending the enterprise to incorporate all stakeholders, including customers, partners, employees, regulators and investors, is a requirement for improved performance.

This paper discusses how organizations have turned to information technology to extend the enterprise. It highlights the challenges that are faced when using technology—such as messaging, data content management and identity management—to respond to stakeholder demands for increased access to information and services. Specifically, this paper focuses on how identity and access management solutions can secure digital identities and information in compliance with regulatory guidelines across an extended enterprise.

Identity and access management solutions that secure digital identities and information can help transform your business. This paper will help you to understand how.

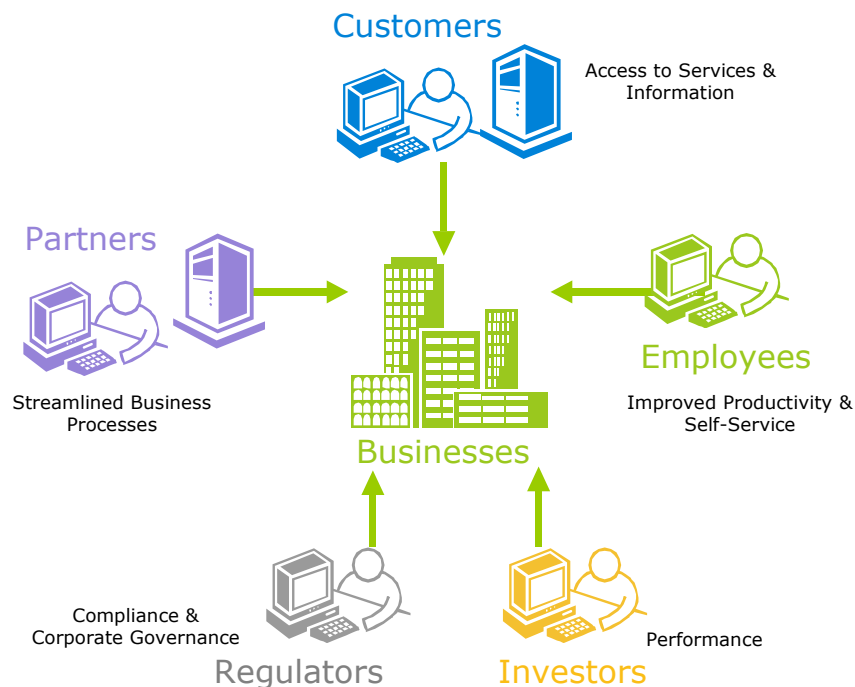
## 2 Extending the Enterprise, Securely

Customers, partners, employees, and even regulators and investors all contribute and are necessary to the success of a business. Creating an environment that encourages all stakeholders to achieve synergies, improve efficiencies and streamline business processes can help to establish competitive advantages and generate an impact on overall business performance.

Organizations are turning to technology—specifically, messaging applications, Web portals, and Web services—to create an extended enterprise that enables:

- New services
- Faster time-to-market
- Broader market reach
- Lower costs
- Increased productivity
- Streamlined processes
- Faster, improved decision-making

However, few business opportunities come without challenges. Opening up access to the information and services that will enable business stakeholders to improve business performance requires the ability to **secure digital identities and information** through the messaging, data and identity management solutions used across the extended enterprise. Further to this is the ability to **audit** the use and enforcement of policies that govern the actions of the enterprise and its stakeholders.



**The Extended Enterprise:** Meeting Stakeholder Demands for Greater Access to Services, Systems and Information

## 2.1 Business Requirements: Identity and Access Management

Ultimately, businesses and governments interacting with stakeholders have the following fundamental requirements:

- They have to **know who they are dealing with** to provide integrity for all types of information, including transactions;
- They **need privacy** for personal information (to prevent issues like identity theft) **and confidentiality** for other types of sensitive information (such as business plans, partner agreements, customer lists, and more); and
- They need control over and visibility into who has access to what, and how they are using it **so that policy can be enforced**, efficiencies maintained and activities **audited**.

These essential requirements exist regardless of whether interactions occur in the physical or digital world.

### Identity and Access Management

- Connecting identities to information
- Providing for integrity of information
- Controlling access to sensitive information
- Protecting the content of information
- Centralizing policy management
- Auditing the enforcement of policy
- Improving corporate governance through a strong information security governance framework

Granted, not all transactions and information require the same levels of security for identity and access management. The steps to extending an enterprise are often taken gradually, starting with simple improvements such as providing access to unprotected and unrestricted information in the form of Web page content. Or, as in most organizations, using e-mail communication as a means to share non-sensitive information.

As enterprises add services and increase the value of the information shared electronically over internal and external networks (like the Internet), the requirements for securing digital identities and information also increase.

For example, selling commodities such as books over the Internet requires a different level of security than other business transactions such as: sending and receiving patent submissions; requesting approval of new drug or medical advances; or, controlling corporate finances over the Internet.

Likewise, the need to audit and track the accountability of data and transactions increases as the sensitivity and importance of the associated information increases. Additional factors including government regulations such as HIPAA, Gramm-Leach-Bliley, Sarbanes-Oxley and California SB 1386 also dictate the level of visibility that is required to maintain centralized control and enforcement of corporate policy.

Recognizing the need to establish strong corporate governance practices via an information security governance framework in a digital world, while maintaining centralized control and auditing the enforcement of corporate policy is the first step towards realizing the productivity benefits of the technologies used to extend the enterprise. The next step is to determine the technologies that will make it possible for organizations to extend their enterprise by securing digital identities and information over

the Internet and enterprise networks while maintaining strong corporate governance practices that comply with regulatory guidelines.

## 2.2 Traditional Approaches to Security Fall Short

To adequately secure their networks and online transactions, enterprises and governments need to deploy a variety of IT security products and capabilities.

Traditionally, most organizations have focused primarily on securing the perimeters of their networks by using firewalls, intrusion detection, and anti-virus software. While each of these types of security is important for protecting networks from malicious intruders and software, none of them is effective at enabling businesses and governments to transform interactions with customers, partners, and employees to help drive new opportunities for productivity, revenue, and cost-effectiveness.

**Traditional approaches** to security—firewalls, intrusion detection and virus scanning software—typically stop protection at the perimeter of the enterprise.

They **fall short** of delivering the class of security required for the identities and information used across an extended enterprise.

Specifically, these traditional approaches to security are not effective at helping organizations be more productive in managing relationships and executing transactions beyond the four walls because they do not identify and help hold accountable the different identities taking part in transactions and communications. On the Internet and enterprise networks, individuals, groups and systems must use **digital identities** to represent who (or what) they are to the application or system that they are using to perform a specific task, transaction or communication.

## 2.3 Securing Digital Identities and Information

To explain why digital identities are so important, let's first discuss the essence of every business and government—relationships and transactions. Every organization exists to manage relationships and execute transactions with a variety of constituents, such as customers, partners, and employees.

Digital identities are critical for securing digital information. You have to confidently authenticate someone to provide them with authorized access to sensitive information, whether that's through authorization or encryption software. It is easy to secure information if you have no desire for anyone to access it (of course, this is not very useful)—the hard part of information security is making sensitive information only accessible to those authorized to see it.

Without **digital identities**, organizations cannot safely manage online relationships and transactions. Simply put, you have to know who you are dealing with in order to manage a relationship and execute a transaction. Digital identities are an important enabling capability for organizations to leverage so that their investments in technology are more productive.

Securing digital identities and information is key for organizations to be able to protect brand equity, trust and financial assets in a digital world.

Technically speaking, digital identities and security technologies need to enable the following **security services** for organizations to manage relationships and execute transactions over the Internet and enterprise networks:

- **Authentication** to determine whether users accessing applications and information are valid;
- **Authorization** so that information is only accessible to those that should have a right to see it;
- **Digital signature** to generate information that can be used to improve accountability; and
- **Encryption** to protect information so that it remains private and confidential as it travels across the network and wherever it is stored.

Entrust is a leader in securing digital identities and information to enable these security services across a broad range of applications and platforms. Through these capabilities, Entrust identity and access management solutions are specifically designed to securely manage relationships and transactions. These solutions can enable customers to leverage enterprise networks and the Internet to help transform their relationships and transactions with customers, partners, and employees in new and exciting ways.

## 2.4 Identity & Security Management

Most significantly, digital identities must be deployed and managed in a way that: allows security services to be delivered with consistent and auditable policy; is low cost to administer; and, is easy-to-use. This is the hard part about securing digital identities and information.



As digital identities evolve through a typical user lifecycle, there are several potential roadblocks that need to be averted so that security is manageable and enforceable. It must be transparent and easy for users and tightly integrated in the applications that they use everyday. For administrators, it must be automated, efficient and able to provide a strong return on the security investment.

Entrust products can allow an organization to implement a **unified approach to managing digital identities and information security** across a wide variety of solutions. This unified approach can result in reduced complexity with increased consistency and policy enforcement across applications, which in turn, can result in **ease-of-use** for users (for example, users have a single password and digital identity across solutions) and **cost reductions** for administrators (for example, much of the user administration occurs automatically and transparently in Entrust solutions and there are self-service user administration capabilities available for organizations to leverage as they see fit).

To realize a better return on extending the enterprise through technology, comprehensive identity and security management must be:

**Easy to Deploy:**

- Centralized and automated rule and role-based provisioning of identities to users, applications and devices;
- Automated enrollment with little application impact—the easier it is to enroll, the faster the deployment and the more effective and less expensive the security implementation; and
- User self-service and automated administrative workflow can simplify deployment processes and help reduce help-desk calls to lower costs.

**Easy to Use:**

- Using identities consistently to secure information across a broad range of applications and platforms;
- Transparently adding security to applications to reduce complexity, encourage use and help lower help-desk costs; and
- Enable single sign-on and password synchronization in addition to role- and rule-based access to information across applications, Web domains and platforms.

**Easy to Manage:**

- Centrally and automatically manage identity information—manage identity information across heterogeneous systems and environments while improving timeliness and accuracy; and
- Managing identities through their complete lifecycle. Whether the digital identity is a simple username/password combination, digital certificate, smart card or token, the complete lifecycle of that identity should be easy to manage. This includes creating, issuing, deploying, revoking, recovering and updating user identities.

The best-in-class levels of digital identity and information security provided by Entrust's solutions can help enable organizations to fully realize and unlock the true productivity promises of the various technologies they are deploying—ultimately enabling businesses and governments to truly transform themselves.

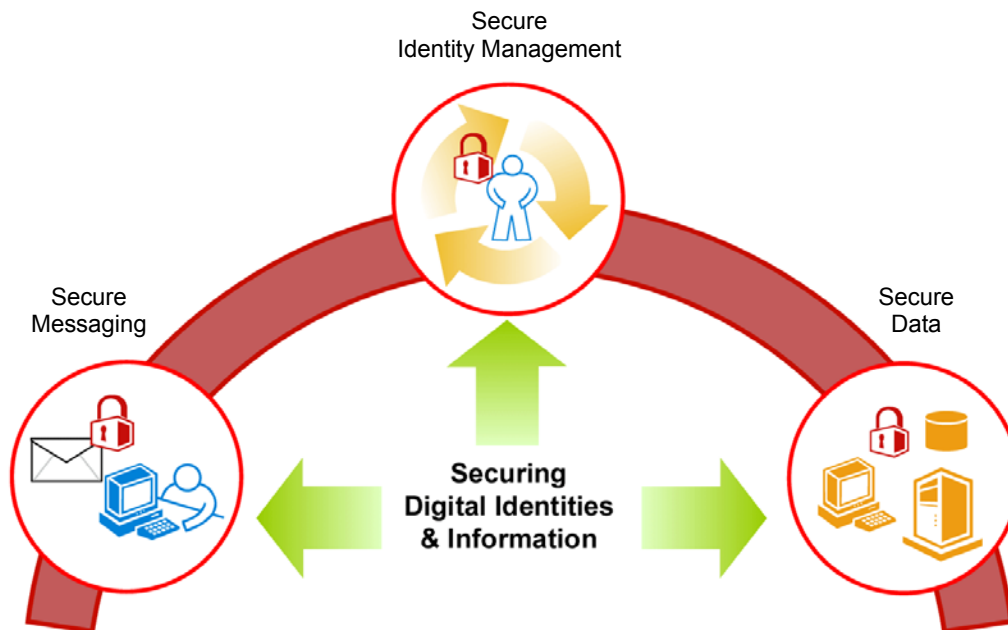
The remainder of this paper will demonstrate how Entrust solutions can help enable transformations that unlock the promises of key technologies.

### 3 Making the Most of Internet & Enterprise Networks

As previously mentioned, business is about making decisions. The faster and more accurate the decisions, the better a business can perform. We use technology to extend the enterprise to achieve tighter integration with customers and business partners. We use the Internet and enterprise networks to foster closer relationships and improve communication with enterprise stakeholders. Desktop applications, Web portals and Web services can be used to achieve faster, improved decision making as an enterprise:

- Offers new services
- Achieves faster time to market
- Broadens market reach
- Lowers the cost of operations
- Streamlines processes and increases productivity

Securing the digital identities and information used in enterprise applications and environments can help eliminate roadblocks and open the door to increased return from the investments made in these technologies. Entrust delivers solutions to cover a broad range of technologies organizations are using today, and planning to use tomorrow.



### 3.1 Secure Messaging

Desktop applications such as e-mail communications, when used by employees, can increase productivity, streamline business processes and reduce costs. Entrust enables secure messaging by delivering security to a wide variety of desktop applications including:

- **Email** applications such as Microsoft Outlook and other S/MIME capable e-mail products to enable encryption and digital signature of messages and attachments



#### 3.1.1 Secure E-Mail

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?

If any of these issues are holding back the leverage you could get out of e-mail, Entrust's Secure Messaging Solution offers an answer that can help enable a business to transform its use of e-mail to **increase productivity**. To unlock the promise of e-mail, Entrust enables organizations to encrypt and digitally sign e-mail messages 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.

Entrust's 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 use of digital signatures, recipients of a message can be more confident in the authenticity and integrity of the communication.

To learn more about how the Entrust Secure Messaging Solution can transform your business or government organization, visit <http://www.entrust.com/solutions/messaging>.

## 3.2 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 solutions 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:

- **E-forms** to secure the workflow and apply digital signatures to Adobe forms, Adobe PDF documents and other Web-based forms; and
- **Desktop files and folders** in Microsoft® Windows™ environments.

### 3.2.1 Secure E-Forms

E-forms can provide organizations with significant opportunities to reduce costs and improve productivity by moving high-value processes online. E-forms represent an excellent technology for managing relationships and executing transactions. 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. The **cost savings** potential is real for almost every type of organization.



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. These two benefits of digital signatures are essential for enabling secure e-forms.

In addition to digital signatures, some types of information included in e-form documents are either private or confidential. Through Entrust's encryption capabilities, users can easily protect the **privacy** of sensitive information so that it is only accessible to authorized individuals.

To learn more about how Entrust security for E-Forms can transform your business or government, visit <http://www.entrust.com/solutions/eforms>.

### 3.2.2 Secure 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 even 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.

Entrust's Secure Data Solution for the desktop **secures sensitive and valuable information** stored on computers, mobile devices and corporate networks. It makes it possible to easily encrypt documents that contain sensitive corporate information. With its security measures, Entrust makes file security even more reliable than previous paper-based processes, to:

- 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; and
- Set certain documents or folders to automatically encrypt, relieving the user or administrator from the responsibility of remembering this task.

And, because Entrust Secure Data Solution is centrally managed, an organization can:

- Enforce certain document security policies throughout the user base;
- Access intellectual property that was encrypted by an employee that is no longer with the organization;
- Issue and maintain the invisible digital IDs needed for proper identification of people accessing secured documents—in a way that is not onerous on the IT team or the users themselves; and
- Leverage the same technology to secure other processes they commonly use.

To learn more about how Entrust secure data solution can transform your business or government, visit <http://www.entrust.com/data/index.htm>.

### 3.3 Secure Identity Management

No two users have the same identity, rights and responsibilities. Your technology environment is likely an uncountable mix of applications, platforms and data types. And, 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. You are also faced with corporate and legislative requirements around governance, accountability, and privacy.

This is identity management. Add to this the **sensitivity and importance** of protecting the identities and information of your business and you need a secure identity management solution.



Entrust Secure Identity Management Solution can increase security, improve productivity and help **lower the cost of your operations**.

A refresher on the security challenges for Web portals and Web services helps illustrate the need for securing digital identities and information across not only client-server, but also Web and Web services environments, as organizations extend their business reach online.

### 3.4 Security for Web Portals and Web Services

The widespread use of Web portals represents one of the most significant advances in technology productivity over the last decade. The benefits of Web portals focus primarily on enhanced services delivered to customers, partners, and employees in a cost-effective manner. These services can help strengthen relationships and streamline business processes to increase transaction rates.

Without adequate security, however, the benefits of Web portals are limited. With adequate security, Web portals provide organizations with a seemingly endless variety of opportunities to transform their businesses.

Similarly, the next wave of computing for the IT industry will be focused on addressing the needs and challenges of business integration using Web service architectures and technology. Organizations that are able to leverage Web services to quickly integrate their business processes within their enterprises and with their business partners and customers will benefit from the **efficiencies of automation and faster customer service**.

Business integration is an evolution of previous computing models. Mainframe computing first introduced the ability to centralize and automate electronic processing of transactions. Client/server computing allowed for decisions and processing to be moved closer to the individual. E-business and the Internet made information and commerce readily available to employees, customers and suppliers.

Web Portals have allowed companies to personalize the information based on individual and role; essentially integration of information for the individual. Now, Web services provide a comparable level of connectivity to business applications.

By building on widely accepted standards that enable easier connectivity between applications, Web services can simplify the development of business-to-business applications, reducing time-to-market and greatly improving the ability to change these applications over time. At the same time, the security mechanisms required for these applications must be sufficient to protect the sensitive and valuable transactions that will use Web services.



### 3.5 Entrust Secure Identity Management Solution

The Entrust Secure Identity Management Solution consists of a comprehensive suite of market-leading identity and access management products, which, in combination or deployed in modular stages, help organizations easily and securely manage identities and access to information for users, applications and devices, while decreasing costs.

It can also improve the ability of organizations to enable legislative and corporate governance compliance. Supporting a broad range of client-server, Web and Web Services environments, the solution makes it easier to securely access applications and information over the Internet. Through best-of-breed capabilities, the solution is easy to deploy and operate, includes secure administration, and can cost-effectively scale to address large user populations.

It includes the following aspects:

- **Strong Authentication:** Authentication using digital identities provides a much stronger form of authentication than username/password, allowing organizations to achieve more effective internal controls. Strong two-factor authentication to desktops, VPNs, WLANs and Web Portals is also available.
- **Authorization and Single-Sign-On:** This area provides methods for addressing the needs and challenges of business integration using Web service architectures and technology and addresses 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.
- **Provisioning:** For centralized identity administration that can help reduce administrative costs and provide comprehensive, secure administration and audit of user identities and access controls.

#### 3.5.1 Strong Authentication

Strongly authenticating users can help organizations in many ways, including reducing costs by moving sensitive applications online. At the same time, strong authentication is an effective way of implementing internal controls, so that only authenticated users are accessing applications and data.



The Entrust Secure Identity Management Solution offers organizations a broad range of authentication capabilities, which enable organizations to match their level of security investment with their security requirements.

The solution offers the following capabilities for strong authentication:

- **Digital Identities** using Entrust TruePass™ Web security or Entrust Entelligence for the desktop environment. Authentication using digital identities provides a much stronger form of authentication than username/password. This easy-to-use, strong authentication enables organizations to confidently deploy high-value applications because the user identity is well protected and that the authentication is strong and secure. For example, it can be determined who is interacting with your Web portal, which is a key issue when deploying higher-value services that involve sensitive information and business processes. Transparent lifecycle management of identities, as well as the ability to encrypt and digitally sign files, is provided.
- **USB Tokens** work seamlessly with Entrust Digital IDs to enable strong two-factor authentication to desktops, VPNs, WLANs and Web Portals. Two-factor authentication is based on something you know (e.g., PIN) and something you have (e.g., a token). By requiring two independent elements for user authentication, this approach significantly decreases the chance of unauthorized information access. As a result of collaboration with Rainbow Technologies, Entrust distributes the Rainbow iKey 2032 tokens as Entrust USB Tokens.
- **Digital Signatures** on Web forms through Entrust TruePass. To enable accountability and integrity for Web transactions, Entrust TruePass provides an easy-to-deploy solution for digitally signing Web-based information.
- **Strong, End-to-End Protection of Information** using Entrust TruePass™ Web security. To protect private or confidential information, Entrust TruePass encrypts information at the browser and the information remains protected from the browser through to back-end systems where it can be stored in a secure manner.
- **Standards-Based Authentication (via SAML) for Web Services** through the Entrust® Secure Transaction Platform helps deliver the fundamental security capabilities that can help enable Web services transactions.

### 3.5.2 Authorization and Single-Sign-On (SSO)

The ability to authorize specific access rights for applications and data can play a key role in strengthening the internal control structure of an organization. Whether on the desktop, through the Web, or via a Web service, identities are used to access sensitive information and as such, must be controlled. At the same time, implementing an unruly set of procedures can increase costs, as users struggle to work within corporate policy. By providing the ability to log-in once and enjoy subsequent single sign-on to the applications and data that a given user is authorized for, organizations gain the benefits of more effective internal controls, with the ability to increase service levels for users.

Concurrently, implementing a central point of authorization can help enable organizations to drastically reduce the cost of supporting multiple applications that must adhere to corporate policy.

Entrust delivers the following capabilities for authorization and SSO:

- **Policy-based Access Control and Web Single-Sign-On** through Entrust GetAccess™ software. Entrust GetAccess protects sensitive information and applications on Web portals through authentication and authorization capabilities. Users accessing Web portals protected by Entrust GetAccess identify themselves using one of a variety of supported single sign-on authentication methods, including username/password and digital identities. Once logged in, users can see a personalized view of authorized services and information they can access.
- **Enterprise Single-Sign-On** with Passlogix v-GO SSO enables Entrust to provide customers with a comprehensive 'best-of-breed' enterprise single-sign-on solution that extends across client-server and Web environments. It addresses the need for a simplified user log-in experience on the desktop that can help allow organizations to transform their business by reducing help desk costs and enhancing the security of password management. The technology provides users with a single secure authentication point for a broad range of Windows®, Web, proprietary and host-based applications without requiring complex application integration. It supports a broad range of authentication methods, including Entrust digital IDs, Entrust USB Tokens, and smart cards, and is seamlessly integrated with the other components of the Entrust Secure Identity Management Solution. As with all components of the modular solution, it is available as a standalone purchase from Entrust.

To learn more about how Entrust authorization and SSO capabilities can help transform your government or business, visit

[http://www.entrust.com/identity\\_management/enterprise\\_value.htm](http://www.entrust.com/identity_management/enterprise_value.htm).

### 3.5.3 Identity Provisioning

In April 2003, Entrust announced the planned integration of Sun Identity Manager (formerly Waveset Lighthouse) with the Entrust product portfolio. The move reflected an increasing desire among governments and businesses to deploy integrated identity management offerings that can help reduce administrative costs and provide comprehensive, secure administration and audit of user identities and access controls. Entrust leverages Sun Identity Manager for centralized identity administration. It can securely and efficiently deploy and manage identities across an enterprise, and can deliver automated identity provisioning, centralized password management, single-step identity profile management, robust auditing of the identity infrastructure and flexible workflow.

For application and device identities, Entrust Certificate Services delivers automated lifecycle management of digital IDs that are used for subsequent authentication and authorization.

To learn more about how Entrust provisioning capabilities can help transform your business or government organization, visit

<http://www.entrust.com/partners/solutions/119.htm>.

## 4 Consistent Security Across an Extended Enterprise

We have seen that identity and access management solutions make it possible to secure digital identities and information in a broad range of applications. The most difficult part about deploying, using and managing digital identities is implementing security in such a way that it is **easy-to-use, consistently applied, able to enforce policy and easy to audit**.

Entrust solutions implement the following identity and security management functions to help simplify deployment and help **lower the cost of extending your enterprise**:

- Centralized definition of identity and security policy;
- Real-time, automated enforcement of policy across applications, platforms and services;
- Security for administrators and workflow to help provide for accountability when managing digital identities;
- Delegated administration and automated workflow to share and decrease the administrative functions across work groups, or with customers and partners;
- User self-service for easier deployment and ongoing identity and account maintenance to improve accuracy of data and quality of service;
- Transparent security and lifecycle management of digital identities to encourage use, enforce policies and make security easier-to-use; and
- Implement standards-based and readily available technologies to make it possible to leverage security across new applications and environments.

## 5 Customers Experiencing a Transformation

For more than a decade, Entrust customers have leveraged security solutions to enable more than just protection. Entrust solutions have helped them to:

- **Save time:** streamlining business processes cutting weeks to days, hours to minutes;
- **Cut costs:** lowering the cost of security administration, reducing and replacing costly paper processes, achieving ROI on security;
- **Decrease risk:** securing digital identities, information and transactions with world-leading security technologies; and
- **Increase productivity:** increase the potential of Internet and wireless connectivity, without unnecessary risk.

Entrust would like to help you get more from your security investment.

Contact us at 888-690-2424 or visit <http://www.entrust.com> to begin your transformation.

Visit <http://www.entrust.com/success> to read the customer experiences of these and other Entrust Customers:

- Bank of Bermuda
- Blue Cross Blue Shield Of Michigan
- California Highway Patrol
- Catholic Healthcare West
- Chase Manhattan Bank
- China Financial Certification Authority
- Compaq Computer Corporation
- Department of Energy (DOE)
- Department of Treasury
- Egg
- Enel Group System Integrator (Enel.it)
- Federal Energy Regulatory Commission (FERC)
- Government of Canada
- Human Resources Development Canada
- Hutchison 3G
- IDX Systems Corporation
- ING DIRECT
- Investment Review Division of Industry Canada (IRD)
- Kaiser Permanente
- KPN
- Lloyds TSB
- Mackenzie Financial Corporation
- Novartis
- Pacific Northwest National Laboratory
- People's Bank of China
- Perot Systems
- Public Works and Services Canada
- Québec Ministry of Justice
- RCMP
- Schlumberger
- SILA Communications
- Southampton City Council
- Southwest Border States
- State of Florida Department of Community Affairs
- State of Illinois
- TDC (TeleDanmark Communications)
- Telia AB
- Thomson Multimedia
- Trac Medical
- U.S. Federal Bridge Certification Authority
- U.S. Patent and Trademark Office
- UK National Health Service
- Vodafone Corporate
- ZebSign

## 6 About Entrust

Entrust, Inc. [NASDAQ: ENTU] is a world-leader in securing digital identities and information. Over 1,400 enterprises and government agencies in more than 50 countries rely on Entrust solutions to help secure the digital lives of their citizens, customers, employees and partners. Our proven software and services help customers achieve regulatory and corporate compliance, while turning security challenges such as identity theft and e-mail security into business opportunities. For more information on how Entrust can secure your digital life, please visit: [www.entrust.com](http://www.entrust.com).