

Entrust[®] Securing Digital Identities & Information



**Securing Your
Digital Life**

Making the Connection

Extending the Extranet to Drive Costs Down and Increase Competitive Advantage

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. Lighthouse is a trademark of Waveset Technologies, Inc. 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. SUCH 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, OR FITNESS FOR A SPECIFIC PURPOSE.

TABLE OF CONTENTS

EXECUTIVE SUMMARY	1
MAKING THE CONNECTION	1
EXTENDING THE EXTRANET: RISK VS. REWARD	4
INCREASING EFFICIENCY & IMPROVING SERVICE.....	5
WEB SERVICES NEED SECURITY.....	5
INFORMATION SECURITY GOVERNANCE IS THE LAW	5
ENTRUST SECURE IDENTITY MANAGEMENT SOLUTION: SECURING THE CONNECTION	6
AUTHENTICATION	9
AUTHORIZATION AND SINGLE SIGN-ON (SSO).....	11
IDENTITY PROVISIONING	13
CONNECT TODAY	13
CONNECT TODAY	14
ABOUT ENTRUST	14

"As enterprises externalize their business processes over the Internet to customers and trading partners, they have expanded the number and types of users with which they must contend. Accordingly, more users need access to IT resources; platform environments will remain complex and heterogeneous; and Web services are driving the need to manage transactions, as well as user access to IT resources."

Gartner "Identity and Access Management Defined" November 2003

Executive Summary

Organizations today are looking for ways to more effectively connect with customers and partners. Although many have initiated projects around creating and serving external users through an Extranet, the ability to manage the growing number of users in a cost-effective manner has introduced challenges that must be addressed, including user self-service for enrollment and password management. In addition to users, enterprises are looking to connect business systems together, allowing partners and suppliers to go deeper into the organization than ever before. While options like Electronic Data Interchange (EDI) do exist, the importance of better connecting with customers and partners is forcing businesses to also look for other flexible options that deliver value and agility.

The task of better connecting with customers and partners is constrained by two key points of pressure. First, in the face of recent corporate scandals and a disturbing increase in identity theft, governments have enacted legislation that puts in place specific requirements about how an organization deals with electronic information, whether corporate or personal. Second, investors are demanding both increased corporate performance as well as increased corporate governance. In addition to complying with the legislated guidelines, investors are looking for clear signs that all business undertaken by an organization is in the best interests of that organization, not a few individuals. Addressing these pressures while still leveraging the Extranet to extend the enterprise is a balancing act that almost every organization struggles with as they strive to connect with customers and partners.

With the widespread acceptance of Extranets as effective vehicles to serve customer and partner users, there are new opportunities to extend the existing infrastructure to connect business applications. Web services applications are a cost-effective and agile way of connecting partner applications with the enterprise, negating past requirements for dedicated inflexible connections. The biggest challenge of Web services today is the fact that, by themselves, they are inherently insecure. The ability to connect with partners through Web services means that Web Services applications and network devices may be transacting business on your behalf or with your organization—with potentially no user ever involved. This new reality necessitates the secure management of application and device identities that will be used in a business transaction for both authentication and authorization. Leveraging these key capabilities can enable an organization to realize the benefits of Web

Services applications while balancing the risk of transactions being conducted without human involvement.

In addition to the demands for increased corporate performance and better service, organizations are also faced with intense pressure for increased accountability, driven by tough legislation and corporate governance mandates. The situation has led to several major laws - including Sarbanes-Oxley, HIPAA, FISMA, the EU Data Directive, and California SB 1386 - that require the strengthening of internal controls and information security governance. Driven by recent corporate scandals and the dramatic rise in information and identity theft, these pieces of legislation have forced organizations to examine how they can best comply with legislation and corporate governance imperatives without significantly impacting business performance.

Key to the success of a compliance initiative is a broad understanding that information security governance is not just a technical issue that can be addressed by the IT organization. It is a corporate governance issue that must be addressed by CXOs (i.e. CIO, CFO, CEO) and Boards of Directors, and must be then implemented and enforced at all levels of the organization. And in today's economic climate, the issue must be addressed in both a timely and cost-effective manner.

Overcoming these challenges to run a competitive, efficient business requires entirely new ways of managing the myriad of relationships that are essential to a business. Central to success is the concept of secure identity management, which can be described as the management and administration of how identities are provisioned, managed, and used on the extended Extranet.

The Entrust[®] Secure Identity Management Solution is a comprehensive, highly scalable solution that can help organizations connect with customers and partners efficiently through both Extranet and Web services applications. The solution delivers a modular set of authentication, authorization, and provisioning capabilities that help lower the cost of managing user, application, and device identities across heterogeneous, complex environments. Through proven best-of-breed capabilities, the solution can improve return on investment for organizations looking to more effectively connect with customers and partners, providing rapid deployment, easy and secure administration, and scalability to address large user populations.



Making the Connection

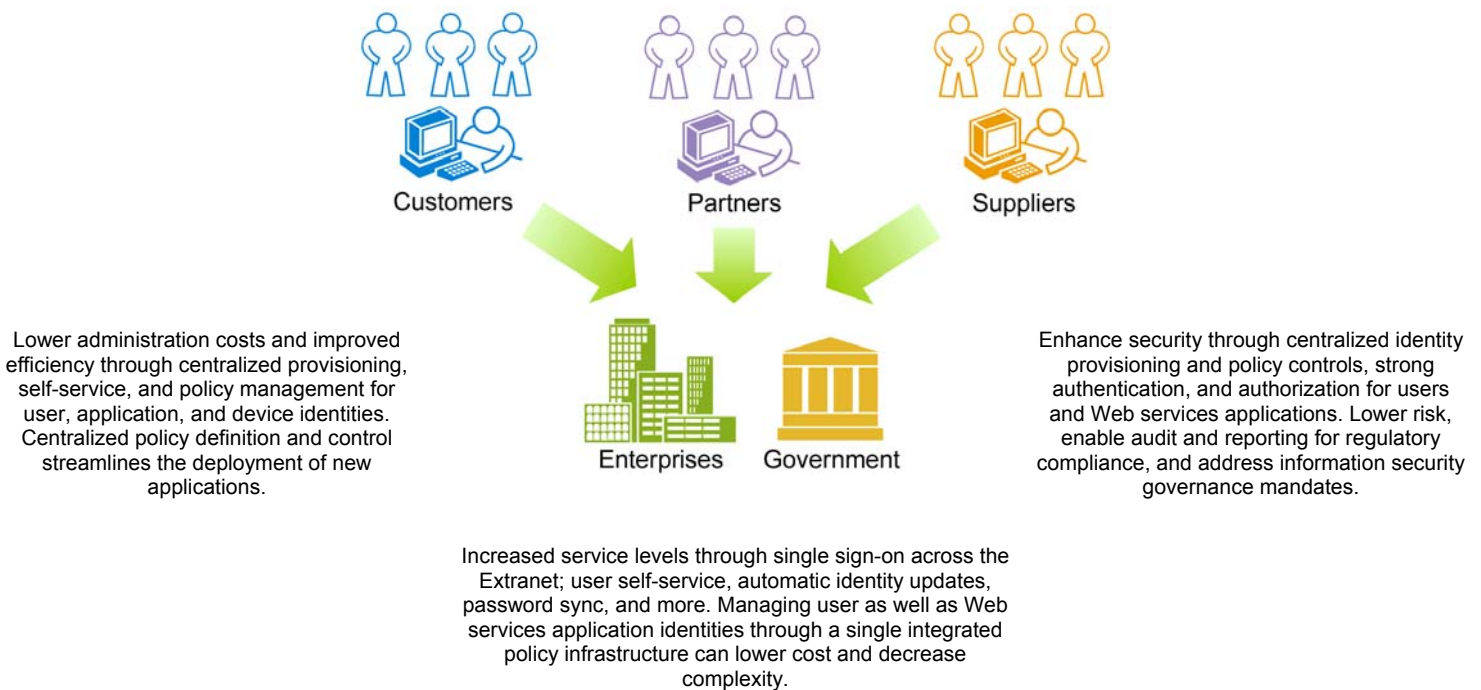
Organizations today are feeling intense pressure to explore new ways to lower the costs of doing business. Already leveraging the Internet to streamline business processes, they are feeling increased pressure to better connect with customers, partners, and suppliers who are demanding real-time, personalized access to information. Whether this means allowing partners to deeply integrate with their supply chain management system, or allowing customers to access confidential account information online, organizations must effectively extend the boundaries of their enterprise to remain competitive. At the same time, the requirement for compliance with hard-hitting legislation is making organizations pay close attention to how they control their business systems.

Extending access to business applications through the Extranet means that organizations must be able to securely deploy and manage identities for all users, applications and devices involved in business transactions – a task that can be very difficult across a large diverse

identity population. At the same time, those same organizations need to be able to control how and when those identities are used in e-business transactions. This means that the ability to centrally control via policy how an identity is authenticated and subsequently authorized for what that identity can do is critical. Finally, organizations must maintain the privacy of user data, while providing accountability for transactions undertaken in their systems.

Leveraging the Extranet as a single portal for users and applications alike can enable organizations to have a central point of both policy definition and enforcement. It can serve as a single infrastructure to support connections with customers and partners, regardless of whether the connection is with individuals or Web Services applications. Extending the Extranet to serve both users and Web Services applications can deliver both increased service levels and reduced costs, enabling organizations to realize competitive advantage through the way they connect with both customers and partners.

Figure 1: A secure identity management solution can enable organizations to more effectively connect with customers and partners





Extending the Extranet: Risk vs. Reward

As enterprises leverage the Extranet to better connect with customers and partners, there are some key challenges that will need to be addressed in order to address the risks of making this connection with the rewards of doing so.

Increasing Efficiency & Improving Service

Doing more with less. A large contributor to the challenge of securing enterprise information exposed through the Extranet is the fact that organizations want to increase service levels and simultaneously need to reduce costs to affect the bottom line. As the number and types of customer and partner identities continue to rapidly grow and change, the need to securely manage those identities grows with it. As a result, IT has to make the process of managing identities and enforcing policy significantly more efficient. More importantly, IT must find ways to do so within the guidelines set out by information security governance policies. This all needs to happen with little disruption to existing business processes and with no compromise to organizational security. Finally, IT purchases must increasingly provide a solid return-on-investment (ROI) in order to get approved, purchased and implemented.

Web Services Need Security

Exposing sensitive information is not an option.

Connecting with customers and partners through Web services applications can deliver tremendous benefits to deploying organizations, including cost savings and rapid application development. However, the inherent insecurity of sending information across the Internet means that these applications connecting business systems together must be secured. This includes being able to strongly authenticate external applications that are reaching deep into an organization's business systems. It also means being able to authorize via policy what transactions that external application is able to undertake. Securing these applications is particularly critical, as the value of transactions over a Web Services interface will typically be substantially greater than with a single Extranet user. And without the ability to manage security for both users and Web Services applications through a single point of definition and enforcement, organizations will be incurring both increased cost and risk.

"By 2006, more than 70 percent of new applications will use Web Services in some part of their architecture (0.8 probability)"

Gartner "Predicts 2004: Advanced Web Services Gain Traction", November 12, 2003

Managing identities for applications is critical. With the ability to allow automated transactions between applications

through Web services interfaces comes the fact that there are now identities other than users demanding access to enterprise resources. These identities may not only be numerous, they will also have diverse needs; they all require different levels of access to different applications and data. The result: IT administrators must keep track of more relationships than ever before — and be prepared to respond quickly to changes, both for the security of the organization as well as the maintenance of service for customers and partners.

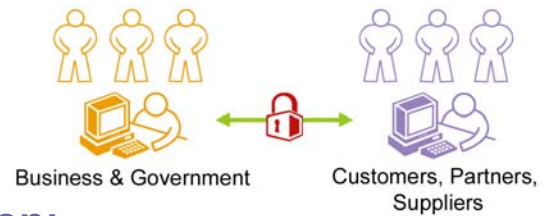
Information Security Governance is the Law

Accountability and audit are legislative requirements. The importance of accountability and security audits in today's organization has never been higher. IT has been mandated to be able to demonstrate the ability to control, audit and report on which identities have access to what resources. Integral to this mandate is the need to not only control what systems identities are provisioned to, but then also to centrally control via policy how those identities are authenticated and what they are authorized to do. Equally important is the security of the central identity administration portal, which must be secured with strong authentication to provide administrator accountability.

Organizations also require the ability to demonstrate an understanding of what has happened within the system, regardless of whether it was a user or an application. Over and above internal audit requirements, legislative measures, including the Sarbanes-Oxley Act and Basel-II, outline accountability requirements for public companies, including the need to implement internal controls for the accuracy of financial reporting.

Without these abilities, organizations risk the possibility of a failed audit and its potential consequences.

Privacy requirements are driven by legislation. As organizations extend the Extranet to better connect to customers and partners, an increasing number of laws have been enacted that mandate security and privacy. Measures like the Health Insurance Portability and Accountability Act (HIPAA), California Privacy SB-1386, the Gramm-Leach-Bliley Act (GLBA), and the EU Data Directive mandate protection of private customer information. With penalties ranging from large fines to jail terms, enterprises and governments must be able to comply with these legislative mandates. And with the real possibility of legal action in the event of a privacy breach, not addressing information privacy may expose the organization to substantial risks and liabilities that far exceed the penalties outlined by the legislation itself.



Entrust Secure Identity Management Solution: Securing the Connection

An effective secure identity management solution should include a variety of capabilities and features that will enable an organization to more effectively connect to customers and partners. The Entrust® Secure Identity Management Solution provides a comprehensive suite of products that allows customers to securely manage identities and control access for transactions with partners, suppliers and customers, through the Extranet or through Web services applications. The solution enables organizations to lower the costs associated with deploying and managing user and Web services application identities while making it easier to securely access applications and information over the Internet. Through best-of-breed capabilities, the solution is easy to deploy and operate, integrates with leading Web applications, includes secure administration, and can cost-effectively scale to address large user populations.

“Effective portal security is best delivered by infrastructure serving the portal and all other applications as a common identity service.”

*Earl Perkins & Craig Roth,
META Group, March, 2003*

Addressing a wide range of secure identity management needs, the Entrust solution includes the ability to support a wide array of **authentication** requirements for both Web and Web services transactions, ranging from user name and password, through digital IDs, to things like USB tokens and smart cards. It also delivers **authorization** and SSO capabilities that enable organizations to centrally manage access policies not only for the Extranet, but also Web services applications. This ability to define and enforce policy through one single interface enables a more streamlined approach to connecting with customers and partners, whether it is through the Extranet or through a Web service application. Entrust also delivers centralized **provisioning** capabilities to address both user and Web service application identity management, including a secure Web-based interface for managing the provisioning process. With this tightly integrated set of products, organizations are able to efficiently manage the complete lifecycle of customer and partner

identities accessing the organization, including not only users, but also Web services applications that engage in transactions with the enterprise. With key features such as secure delegated administration, password management user self-service, and centralized policy enforcement, the solution is able to effectively manage identities and access in a distributed environment.

The Entrust solution supports one of the broadest ranges of applications on the market “out-of-the-box”, helping to lower the cost of deployment for an organization. This includes the ability to provision identities to Entrust® applications, as well as other applications that leverage digital IDs, including Web services applications. It provides the benefit of being able to extend beyond the Extranet, providing centralized identity and access management to enterprise applications employing Web Services to interface and execute transactions. This ability to manage identities across a broad range of applications allows organizations to cost-effectively connect to customers and partners through the Extranet, as well as secure Web services applications.

The Entrust Secure Identity Management Solution is unique in its ability to provide seamless integrated security around the identity administration environment, including strong authentication and policy-based access control for system administrators. The solution extends Entrust’s user management capabilities to include flexible workflow, self-service user management, and automated password synchronization that can make it even more cost-effective for deploying organizations. The Entrust Secure Identity Management Solution also includes additional elements such as customized workflow and smart forms that make it easier to provision Entrust products.

Deployed individually or together, the products that make up the solution are tightly integrated and delivered as a cohesive package, allowing organizations to pick a single starting point as an on-ramp to future capabilities.

Figure 4: The Entrust® Secure Identity Solution includes best-of-breed products that are delivered and supported by Entrust, leveraging Entrust’s best-in-class global service and support team to allow organizations to efficiently deploy the solution.



Authentication

Supporting a broad range of authentication methods across the Extranet, the Entrust solution enables organizations to connect the value of a resource to the level of authentication needed to access it. For many customers and partners, the use of a policy-enforced password may be appropriate and sufficient. However, for more sensitive applications, strongly authenticating users can help organizations in many ways, including helping to reduce costs by being able to move sensitive applications online without an inordinate amount of risk.

Through **Entrust GetAccess™**, the Entrust Secure Identity Management Solution supports one of the broadest ranges of authentication methods for Extranet users on the market today, including Security Assertion Mark-up Language (SAML) v1.1, random number tokens (e.g. RSA SecurID, Safeword) browser certificates (X509v.3), Entrust TruePass™, Entrust® USB tokens, smart cards, and even biometrics.

Entrust GetAccess also supports the ability to authenticate users and applications to non-Web resources, including Enterprise Java Beans (EJBs) and Microsoft .NET applications, making it a central point of policy enforcement for more than just Extranet applications.

The Entrust Secure Identity Management Solution includes the ability to secure the sensitive identity administration portal with integrated strong authentication through Entrust TruePass. This ability to secure the portal is critical, since one of the fundamental underpinnings of security for applications that are managed using a centralized identity management system is assurance of an administrator's identity. Strong authentication is used so that only recognized administrators are granted access to the system, enabling organizations to confidently deploy and realize the benefits of identity management. Verifying the identities of those administering identities and access rights becomes even more challenging when connecting with customers and partners.

The Entrust Secure Identity Management Solution includes a modular set of products that can be used individually or in combination to implement varying levels of authentication for more effective internal controls. For strongly authenticating Extranet users, the solution delivers multiple capabilities for organizations concerned about ensuring the identity of

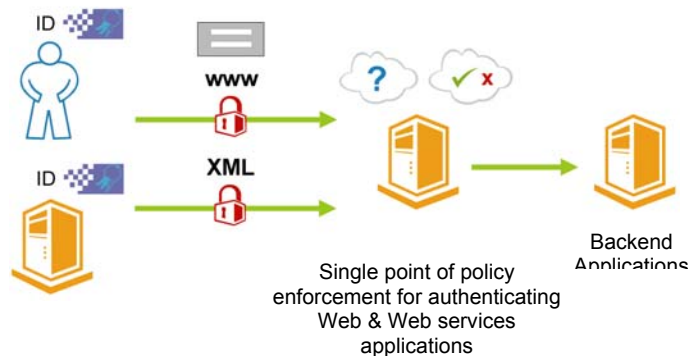
users. **Entrust IdentityGuard™** provides a second factor of user authentication that is designed to help organizations counter identity theft by making it more difficult for attackers to steal user online identities. With Entrust IdentityGuard, users continue to employ their current user name and password, but are also provided with a second physical form of authentication based on an assortment of characters in a row/column format printed on a card. Using a patent-pending challenge and response technique, Entrust IdentityGuard™ can help increase the security of online identities, significantly improving an organization's resistance to identity theft attacks such as phishing.

Entrust TruePass™, which is a “zero-footprint” product that leverages Entrust digital IDs to uniquely identify a user. The zero-footprint capability makes it easier for customers to strongly authenticate, helping to reduce help desk calls and provide a higher level of customer service. With the ability to mandate the use of a digital ID, on a smart card or stored locally, organizations can confidently control access to sensitive applications for customers and partners that are accessing the Extranet. Without deploying any further software or hardware, Entrust TruePass can also be used for applying digital signatures and encryption for enhanced accountability and privacy.

For organizations wanting two-factor authentication with identity storage, the solution includes **Entrust® USB Tokens**. Entrust USB Tokens are designed to securely store an individual's digital ID that is used to strongly authenticate them to a sensitive application.

Extending the Extranet to support Web Services applications is enabled through the use of the **Entrust® Secure Transaction Platform**. Working in conjunction with Entrust GetAccess, it delivers standards-based (via SAML) authentication to Web services applications. Working independently, or in concert with SOAP gateway applications like VordelSecure®, it serves as a SAML authority for Web services applications requiring authentication. As the Entrust Secure Transaction Platform Server works with Entrust GetAccess as its policy definition and enforcement engine, deploying organizations will be in a position to realize cost benefits over competitive offerings through simplified management requirements.

Figure 5: The Entrust Secure Identity Management Solution delivers the ability to support both users and applications authenticating to the organization, leveraging standards-based interfaces to secure sensitive extranet content.



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 through the Extranet, or via a Web Service, identities are used to access sensitive information and as such must be controlled according to corporate policy. At the same time, implementing an unruly set of procedures can increase cost 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 can gain the benefits of more effective internal controls while increasing service levels for users. At the same time, implementing a central point of policy definition and enforcement for both extranet and Web services applications can enable organizations to reduce the cost of supporting multiple applications that must adhere to corporate policy.

SSO and Access Management can yield:

- Improved data management of \$350 per user per year
- Reduced development of security features and user management of \$12,000 per application
- General support improvements of \$70,000 per year

Source: Giga Information Group, "Justifying the 2003 IT Budget: Identity Management Brings Quantifiable ROI to Security", October, 2003

Entrust GetAccess™ delivers policy-based access control and SSO for the Extranet. It is used across the Extranet to secure and streamline access to sensitive information, including the ability to leverage it for securing the user self-service portal. Proven in deployments of millions of users, Entrust GetAccess can also be extended to provide robust authorization controls for both Enterprise Java Beans (EJBs) on leading application servers from IBM and BEA, as well as applications deployed on the Microsoft .NET platform.

Entrust GetAccess provides key features for connecting with customers and partners through the Extranet, including

being able to be easily extended to support Web Services, including:

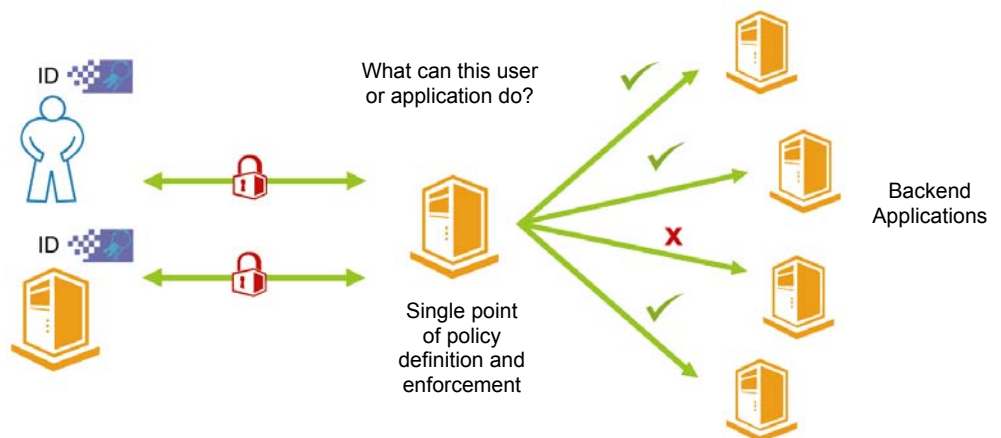
- An unlimited user, per-processor licensing model that allows organizations to more closely tie the value of the Extranet to the amount paid to protect it;
- Centralized real-time session management and single sign-off in a multi-domain environment (supported via SAML) including support for idle and session timeouts, and real-time user revocation;
- Centralized configuration management, removing the need to configure multiple servers and instances
- Employing XACML-based policy for granular authorization and entitlements;
- Demonstrated performance and scalability through real-world multi-million user deployments;
- An architecture employing a single thin run-time approach that is designed to reduce impact on Web server environments for maintenance and upgrade.

"Generally heightened awareness of IT security issues, plus legislative action on IT security responsibility, ensure that Web Services security will not be overlooked as a concern to be addressed."

Randy Heffner, Forrester Research - "IT Trends 2004: Secure Web Services", November 2003

Extending the Extranet to support authorization for Web services transactions is enabled by the **Entrust® Secure Transaction Platform**. Much like authentication, it works in conjunction with Entrust GetAccess to deliver standards-based (via SAML) authorization capabilities to Web services applications. Working independently, or in concert with SOAP gateway applications, it serves as a SAML authority for applications requiring authorization, inside the enterprise or in federated environments. The tight integration between the security mechanisms for both Web and Web Services applications delivered through the Extranet makes connecting with customers and partners, whether users or applications, more cost effective than implementing different solutions.

Figure 6: The Entrust Secure Identity Management Solution delivers the ability to control via policy what a user or application is authorized to do through the Extranet. This includes being able to define not only the strength or type of authentication required, but also what actions can be undertaken once authenticated, for both users and Web services applications.



Identity Provisioning

The Entrust Secure Identity Management Solution delivers provisioning of user identities across Web and Web services environments. For Extranet users, the solution leverages the best-of-breed capabilities of **Sun Identity Manager** to automate the provisioning process and provide key user self-service capabilities. Key to mitigating risk around a centralized approach to user provisioning, the Entrust solution includes strong security around the central administration portal through Entrust TruePass, so that only strongly authenticated users gain access to sensitive identity administration capabilities.

As a part of the identity provisioning process, the Entrust solution includes automated provisioning for Extranet users (partners, suppliers, customers, citizens), as well as automated approval processes using e-mail and Web links for approvers. Streamlining the user management process with automated provisioning can reduce the strain placed on IT staff to keep up with this level of change. Automation also provides visibility into and control over who has access to what, helping to improve the security of the environment, and making it easier to pass security audits. And ultimately passing security audits can help companies comply with key legislation such as Sarbanes-Oxley, HIPAA, and others.

The Entrust solution also provides centralized password management that can reduce the one of the largest sources of costly help desk calls and, at the same time, enhance service and security. For users, being able to change or reset passwords from any Web browser or phone is better than having to call the help desk for every forgotten password. And for the enterprise, the fewer calls

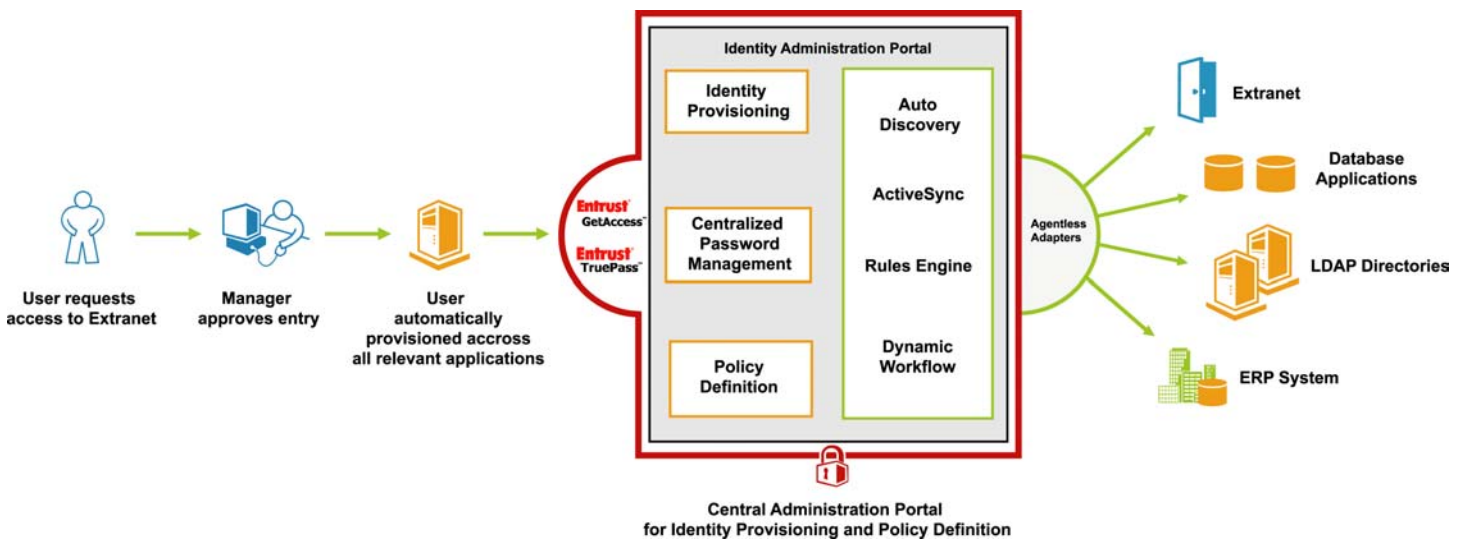
to the help desk, the lower the cost for user support while still delivering increased service.

Sun Identity Manager delivers a dynamic workflow capability that automates the process of making changes in identity data, passwords or access permissions that are executed as a result of rule evaluation. Routine approvals and notifications can easily be automated to fit into how a business works today (as opposed to forcing change).

Addressing two of the key challenges faced by most provisioning offerings, the Entrust Secure Identity Management Solution delivers an 'agentless' approach to deployment, leveraging remote management protocols to connect securely to managed resources, helping to speed deployment and simplify ongoing management of complex environments. The second challenge of centralizing user data from multiple applications is addressed by the fact that the solution only stores basic parts of an identity centrally (i.e. first name, last name, and phone number). All other identity data remains in the relevant application, and is only accessed on demand when needed. This unique way of dealing with user data can help organizations address privacy concerns raised by centralizing user data.

For Web services application identities, **Entrust[®] Certificate Services** delivers automated lifecycle management of digital certificates that are used for subsequent authentication and authorization. Entrust Certificate Services can automatically deliver a certificate to a server application, and then subsequently manage the entire lifecycle, from renewal through to revocation.

Figure 7: From the time a user enters into a relationship with an organization, the Entrust solution begins to **monitor and enforce** that user's access privileges — and it continues to do so throughout the lifecycle of that relationship.





Connect Today

Organizations today are feeling increased pressure to remain competitive while lowering the costs of doing business. As they look for new ways to streamline business processes, they are experiencing an increasing need to find new ways to service customers and partners who are demanding real-time, personalized access to information. Whether this means allowing partners to deeply integrate with their supply chain management system via Web services, or allowing customers to access confidential account information through the Extranet, organizations must effectively extend the boundaries of their enterprise to remain competitive. At the same time, organizations need to manage the identities of the increasing number of end-users that are accessing enterprise applications exposed through the Extranet.

To add to this, organizations need to be able to centrally manage and enforce security policy in order to comply with hard-hitting legislation and corporate governance initiatives focused on mandating corporate governance standards and avoiding risk.

Building on over 10 years of experience satisfying Global 1000 companies, Entrust has assembled a comprehensive solution that is unmatched in the industry, making it the right choice for solving secure identity management needs for the Extranet. It is unique in its ability to manage identities and access across the Extranet and Web services environments, delivering a modular set of authentication, authorization and SSO, and provisioning

capabilities for users and Web services applications. It includes features that enhance security and overall accountability for organizations, including a robust auditing system that enables organizations to review and document identity transactions. The Entrust Secure Identity Management Solution addresses the need to manage large user populations, providing a high performance, scalable solution for addressing identity and access management needs.

The longer an organization waits to adopt an effective secure identity management solution, the greater the cost for supporting the demands of customers and partners through the Extranet. At the same time, waiting also introduces a risk of compromising secure information and putting the company in a state of non-compliance with legislation that can have severe penalties for both individuals and corporations. The Entrust Secure Identity Management Solution delivers a comprehensive set of best-of-breed capabilities for secure, cost-effective control over users and their access to Extranet resources. Furthermore, Entrust services and supports this tightly integrated solution through its best-in-class global support organization, helping organizations to rapidly deploy and utilize the solution. Organizations that embrace the extended Extranet today to more effectively connect to customers and partners can quickly realize cost savings and increased service levels that can ultimately lead to a competitive advantage.

For more information on how the **Entrust[®] Secure Identity Management Solution** can help you to connect to customers and partners through Web and Web Services applications, please visit: http://www.entrust.com/identity_management/

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.