

BUYER'S GUIDE
WEB PORTAL SECURITY SOLUTION

Date: **November 15, 2001**

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.

© Copyright 2003 Entrust. All rights reserved.

TABLE OF CONTENTS

1 ISSUES TO CONSIDER AS YOU COMPARE SOLUTIONS..... 3

2 SECURITY 4

3 PERFORMANCE 6

 3.1 PERFORMANCE - SCALABILITY & AVAILABILITY 6

 3.2 SCALABILITY – ADMINISTRATION..... 7

4 FLEXIBILITY..... 9

 4.1 FLEXIBILITY - INTEROPERABILITY 10

5 SUMMARY 12

1 ISSUES TO CONSIDER AS YOU COMPARE SOLUTIONS

This Buyer's Guide will assist you in comparing the Entrust GetAccess™ solution with other products you may be considering for managing and securing Web access to enterprise applications and services. This guide explains in clear, concrete terms why certain capabilities are important for Internet-scale secure Web portals and how Entrust GetAccess differs from other vendors' products.

There are several broad categories of capabilities and requirements that should be considered in the product evaluation process:

- **Security** – The portal security tool you select will provide a critical component of your overall security solution. It should deliver the level of security needed to provide your users with the online services and applications they need without compromising their privacy and trust, or the integrity of your site and your brand.
- **Performance** - As a portal begins to grow, it is imperative that your infrastructure has the performance capabilities required to scale with this growth. This refers to overall system reliability as well as scalable administration.
- **Flexibility** – Each portal deployment has a varied range of business requirements that must be met for a project and deployment to be successful. In addition, a portal is composed of a broad suite of technology and infrastructure tools. These may include hardware platforms, Web servers, networking devices, application servers, databases, directories, and other components. In order to allow successful deployment, the secure Web portal tool you select must be able to operate in this rich and diverse environment in addition to being flexible enough to accommodate modification and integration to better match your needs.

Each of these categories contains numerous lower level requirements that are highlighted in the following pages. Responses are supplied for Entrust GetAccess. Compare them thoroughly against the capabilities of other products you may be considering in order to determine which product solution is most likely to help you succeed in your portal initiatives.

2 SECURITY

Security is at the heart of online delivery of services and applications via a Web portal. Users will only be motivated to use and return to your site if they are confident that their information is being managed in a manner that they trust. Entrust pioneered the Internet security marketplace, with over 10 years of experience delivering the industry's most robust security solutions. Unlike other vendors, Entrust GetAccess has been designed from the ground up to provide robust security without sacrificing performance.

When comparing the world-class security that Entrust GetAccess provides against other tools, evaluate the following critical security capabilities:

- **Are user sessions centrally managed and/or tracked?**

Entrust GetAccess tracks all user sessions via a centralized Session Management Service (SMS). This allows your administrators to have real-time visibility into the user activity that is taking place on your portal.

- **Does the solution generate session-specific keys for encrypting cookies?**

Because of its unique centralized session manager, Entrust GetAccess encrypts each set of session credentials with their own unique key. This is unlike other products that use the same static key to encrypt all credentials for all users and for all sessions. For those products, the compromise of that single static key (which is vulnerable over time) equates to the compromise of all user credentials.

- **Does the product support single-signoff out of the box? Even across multiple Internet Domains?**

While many products support single-signoff to provide security for users, Entrust GetAccess logs a user out of the system and invalidates their credentials for all Entrust GetAccess secured servers, even those in other domains.

- **Does your Web portal solution verify a user's password against the directory or database every time the user authenticates?**

While competing products only look up passwords against a cache to deliver artificially inflated performance statistics, Entrust GetAccess compares passwords against the persistent security database that you have selected. This validation is performed in an efficient transaction so that you have robust performance to power your site without exposing you to the significant risk of having a user authenticate with an expired or revoked password.

- **Is user information cached at the Web server in order to provided artificially enhanced performance numbers?**

User information of any type is sensitive and should be kept private. Some competing products cache user and privilege information at the Web servers in order to enhance performance. However, this could expose your user data to attack since Web servers typically live in the DMZ, commonly considered to be the most vulnerable point in the corporate network. Entrust GetAccess delivers robust performance without caching any user information whatsoever.

- **Does the product support robust intrusion detection? Does “turning on” this capability incur a performance loss? Does the product support a notification mechanism if the system is under attack?**

Entrust GetAccess provides sophisticated intrusion detection capabilities out of the box. An administrator defines thresholds for failed login attempts as well as a list of security personnel to inform if a potential attack is attempted. Then, if a cracker attempts to break into an account, the system will immediately lock out the targeted account(s) and notify the administrators that an attack is being attempted.

Entrust GetAccess will not only track such activity centrally so that the security mechanism is not defeated, but will also log all suspicious activity so that auditors and security administrators can perform detailed and rigorous analysis to determine where, when, and how often attacks take place.

- **How well does the solution integrate with Digital Certificate-based solutions to offer enhanced security via strong identification, verification (Digital Signatures), and privacy (Persistent Encryption)?**

Many companies are starting to deploy digital certificates to their end users in order to implement stronger security than can be delivered using just passwords. In addition to providing stronger authentication using public-key technology, certificates also make it possible to implement digital signatures that are secure and that are now recognized in legislation in many jurisdictions. Certificates also make it possible for data to be encrypted all the way from the browser to the back end server, thus making it almost impossible for attackers, even ones that are inside the secured network, to access sensitive data.

Many solutions, including Entrust GetAccess, integrate with simple, unmanaged Web certificates that are used for SSL client authentication. However, only Entrust GetAccess integrates tightly with the Entrust TruePass™ portfolio of products to provide transaction signing and encrypting capabilities.

- **Has the product been evaluated or audited by a third-party?**

In addition to the rigorous evaluation Entrust GetAccess typically gets subjected to by most customers, the product has also been audited by the Spectria division of Rainbow Technologies. Consider the following extract from the announcement of the completion of successful testing of successful testing:

The comprehensive testing and assessment process involved examining Entrust GetAccess from multiple perspectives, including architecture, protocols and applications, using Spectria's unique Three-Layer Analysis.

Spectria subjected the Entrust GetAccess solution to rigorous laboratory testing on multiple platforms, in a variety of configurations. “We are confident,” says Bernie Cowens, CISSP, Spectria's Director of InfoSec Services, “that this product meets the highest standards of security.”

In an area as vital as security, make sure that the solution you choose has been successfully evaluated by an independent authority in the area of data security.

3 PERFORMANCE

The solution you choose must be able to perform complex authorizations for millions of simultaneous users and content contributors. It should reduce network traffic by providing single sign-on rather than requiring repeated authorizations. And, of course, it should smoothly accommodate growing numbers of users and applications.

In keeping with customer requirements for highly scalable, highly reliable portal technologies, Entrust GetAccess is designed with a distributed, component-based architecture. This flexible design enables the Entrust GetAccess solution to scale to support a large number of users, resources and concurrent transactions. By simply deploying additional access servers and replicating the Entrust GetAccess services, enterprises can distribute traffic loads and improve the response performance of the entire portal environment. In addition, if any one component fails, the replicated Entrust GetAccess services will continue functioning, providing reliable, continuous performance for critical e-business operations.

To determine whether a solution is reliable and scalable, you need to ask a potential vendor the following questions:

3.1 PERFORMANCE - SCALABILITY AND AVAILABILITY

- **How scalable is the product's structure? Will it scale to millions of users, globally?**

Entrust GetAccess has been deployed to over a million users at several client sites to power B2C portals. In addition, Entrust GetAccess has been deployed to over 200 other customers at various locations across the world in Intranet, Extranet, and Internet-facing deployments.

- **Does the product support replication to increase system performance?**

Entrust GetAccess is engineered to work in replicated environments. Built on top of a standards-based architecture, it supports the deployment of any of its services in multiple instances.

- **Does the product provide automatic fail over? Is administrative action needed? Is this fail over transparent to the end-user?**

In the event of failure of a component of Entrust GetAccess, other components that communicate with it will automatically and transparently fail over to a different instance. No administrative intervention is required and no user information should be lost.

Entrust GetAccess leverages standards-based mechanisms so that the system is stable and available even in the event of certain services, machines, or even data centers becoming unavailable. The system has been designed from the ground up to contain no single point of failure. Each Entrust GetAccess component can be deployed across multiple machines and instances to meet availability requirements.

Furthermore, each component is capable of automatically discovering the location of the services that it requires, even ones that are installed after it has been configured. This means that as your system grows over time and you deploy new instances of services, it is not necessary to go back and re-configure the dozens of servers (front and back-end) that you have already deployed.

3.2 SCALABILITY – ADMINISTRATION

In addition to performance and availability, scalability also refers to the ability to manage and administer an ever changing and expanding user population. It involves things such as browser-based, delegated administration, user self-service, and automated enrollment and provisioning.

Delegation is the answer to making administration scalable. While you want to centralize access policy definition, monitoring, enforcement and auditing, you want to decentralize day-to-day decisions about who has access to what. Without losing control, you need to push such responsibilities into your lines of business, to people working directly with customers and/or developing Web applications. These are the people who can make the best and fastest access decisions.

Designed for efficient management and deployment flexibility, Entrust GetAccess includes a multi-level, delegated administration model. Categories of administrative tasks can be delegated and decentralized, helping to improve response time for user requests and providing multiple points of system control. For example, hotline staff can receive delegated administrative authority to help users with common requests such as forgotten passwords, or resource owners can decide who should have access to their resources. Administration applications enable most tasks to be performed with a few mouse clicks.

- **Are there any logical limits on number of users? Number of resources?**

Entrust GetAccess employs a flexible and extensible object-oriented data model that places no limits on the numbers of users, roles, resources, or other objects in the repository.

- **Does the solution offer a comprehensive browser-based administrative capability out-of-the-box? Is there an extra charge for delegated administration?**

Some vendors offer no user management capabilities as part of their core product offering, choosing instead to charge extra for this basic management capability. Others don't provide browser-based administrative access, mandating you to deploy and manage client-side software for all of your administrators, potentially including those that are geographically separated or that are part of another entity.

Entrust GetAccess offers a comprehensive delegated administration capability out-of-the-box. No client side software is required. This capability is provided as part of the core Entrust GetAccess product and is not an add-on that you need to purchase, manage, or deploy separately.

- **Is it possible to delegate administrative responsibility by group (e.g. Defined administrators can only manage users in a particular department or location)? Is it possible to delegate administrative responsibility by function (e.g. Certain administrators can only reset passwords, others can manage the entire user object, while others still can only manage access to a particular application)?**

Entrust GetAccess provides such administrative scalability through its sophisticated and user-friendly Administration Module. This browser-based GUI allows the administration of every element within the Entrust GetAccess infrastructure (including users, roles, resources, and security parameters). Additionally, the tool empowers administrators via a powerful delegation model whereby administrative privilege(s) can be handed down in two different ways:

By User: This type of delegation allows a higher-level administrator to limit which users a delegated administrator can view. This allows an enterprise to push user delegation out to the particular business partner or department that those users belong to. For example, a super-user for an automotive parts exchange could set up different delegated administrators for Ford and GM. When the Ford administrator accesses the administration tool, he will only see other Ford users. He will not have any visibility into any other users and also will not be able to access any non-user data such as server settings or security parameters.

By Function: Delegation by function refers to the ability to hand down certain pre-specified administrative tasks to a lower-level administrator. Examples of such tasks might be user maintenance, server management, or Helpdesk administration. This allows for the creation of some users who staff a call center and can only reset passwords, and other users who can only manage resources on a particular server, but cannot see any users or other system elements.

Further, it is possible within Entrust GetAccess to use these two types of delegation together in order to create delegated administration models that match the business needs of an enterprise. To extend the example of the parts exchange, it is possible to have several types of administrators within Ford for various functions. A Ford user manager can access full user information and create and modify all of Ford's users. A drilled down Helpdesk administrator might only be able to see Ford contractors (as opposed to all Ford users), and for those users, he or she can only reset passwords.

- **Does the system provide auto-enrollment (self-registration) out-of-the-box? What other self-service capabilities are provided?**

Entrust GetAccess has automated, integrated self-service registrations and subscriptions. Users can self-register and set up a profile immediately. Self-registration includes the ability to map attributes from the authenticating system to attributes in Entrust GetAccess. Examples are: LDAP attributes to Roles, NT Global Groups to Roles and SecurID groups to Roles.

Each supporting self-registration allows the customer the flexibility to pick the self-registration authority and the nature of the role-mapping so that the self-registration can be implemented to support separate, non-cooperative, business units to register a person into a central portal for the Enterprise. For example, one business unit may have its customers in an IBM Secureway Directory (LDAP) and other business unit may have its customers in a Netscape Directory. Customers of the first business unit can self-register to the Secureway, customers of the second business unit can self-register to Netscape. Each business unit can meet its unique requirements by defining the policy on role assignment during self-registration.

4 FLEXIBILITY

No product is going to meet 100% of your requirements out-of-the-box. In order to get a “best-fit” for your needs, you will need a tool that is powerful, but also flexible enough to be molded into your environment. Entrust GetAccess delivers a robust suite of capabilities so that your portal experience remains the way you want across domains, and that it has the necessary hooks and APIs to seamlessly integrate into a variety of applications and workflow environments. In addition, the ability to interoperate with the hybrid technologies used to power portal is critical.

- **Does the solution you're considering provide true Multi-Domain support? Does it perform fine-grained entitlements across domains? Are timeouts, logoffs, and revocations supported?**

Entrust GetAccess provides true multi-domain support for the secured Web portal. Unlike other products that only provide a nominal authentication token for “non-primary” domains, Entrust GetAccess supports entitlements, session management, and user revocation across a large number of Internet domains.

- **What types of toolkits and APIs does the solution provide?**

Entrust GetAccess delivers a complete suite of APIs to provide a broad range of application integration possibilities. Entrust GetAccess APIs are delivered as part of the core product in two separate capability areas:

The Entrust GetAccess UserAPI (implemented in Java) provides programmatic access to the Entrust GetAccess data store, and is commonly used to automate data lookup or admin automation from external applications. This API can be used to create, update, and remove users, or to look up data elements for users.

The Entrust GetAccess CAAS (Client Authentication and Authorization Service) is a toolkit provided in Java and C++ that is used to integrate non-Web applications into Entrust GetAccess. It provides programmatic access to Entrust GetAccess functionality and can be used to perform operations such as user authentication and authorization, session validation, and session revocation.

- **Does the solution provide any “hooks” that allow customization of system behavior? How will the system provide the needed flexibility to help to meet your business requirements?**

Entrust GetAccess delivers a comprehensive set of exit points within the system's operating workflow that allows you to modify what happens at a given point. There are a set of approximately 25 pre-defined “Events” that occur during normal system activity. Examples of Events include successful authentication, failed authentication, user creation, session termination, etc. Entrust GetAccess allows you to write your own “Extensions” to these events to modify the default behavior of the system. Extensions are snippets of java code that you write, compile, sign (for security purposes), and tie to an event. From that point forward, any time that Event takes place, Entrust GetAccess will execute your Extension before returning control back to the system default.

- If you want the user to accept a license or liability screen when they register for an account, you can write the appropriate code and then link it to the onSuccessfulSelfReg event.

- In order to conform to your specific password rules, you can extend the onChangePassword event.
- The onSuccessLogin event is commonly extended in order to dynamically entitle a user for different privileges based on external parameters such as user location, bank balance, time-of-day, etc.
- **How will the system integrate with your legacy applications? With other non-Web applications?**

The Entrust GetAccess CAAS toolkit extends the robust identification, entitlements, session management, and other services provided by Entrust GetAccess, to the non-Web world. Clients have used this toolkit to integrate Entrust GetAccess with Client/Server, Mainframe, and IVR applications. This toolkit can also be used to add security to other transactions such as FTP, Telnet, and streaming media.

- **Is the product fully double-byte enabled? Is it easy to localize for different languages and locales?**

As workforces become increasingly mobile and B2C portals expand their reach worldwide, it becomes more important to allow your end users to interact with you in the language of their choosing. The Web portal solution you choose should be completely localizable so that you can personalize the experience that your users have at your portal, right down to the language in which you communicate with them.

Entrust GetAccess has been deployed to customers all over the world including the U.S, Canada, the U.K., Spain, Germany, the Netherlands, Finland, Sweden, Denmark, and Japan. The system is double-byte enabled so that it is localizable to any language you need.

All Entrust GetAccess HTML that an end user can possibly see is driven from within a sophisticated template framework. In order to support a language, it is only necessary to duplicate the templates within the framework for the target language. When HTML is being rendered for a user, Entrust GetAccess will automatically select and fill the appropriate template corresponding to the user's preferred language. The result is that different users accessing your portal simultaneously will see the same screens, but localized for their language.

4.1 FLEXIBILITY - INTEROPERABILITY

A critical factor to the success of your portal security solution lies in its ability to interoperate with the hybrid technologies that are used to power portal. These technologies include Web servers, directories, application servers, and other infrastructure components that typically complete an architecture.

Determine whether the solution you choose will meet your current and future infrastructure requirements by obtaining the following information:

- **Which Web servers and operating systems does the solution support?**

Entrust GetAccess has broad support for Web servers and platforms. Supported Web servers include:

IPlanet / Netscape Enterprise	Microsoft IIS
Apache	Domino

Supported Web platforms include:

Microsoft Windows NT	Microsoft Windows 2000
Solaris	HP-UX (Q1)
AIX (Q1)	

- **What databases or directories does the solution support?**

Entrust GetAccess supports Oracle and SQL-Server 2000 databases and iPlanet Directory Server, Siemens DirX, and Novell eDirectory for LDAP-based repositories. Additionally, the Entrust GetAccess LDAP PAAM allows you to leverage any LDAPv3 compliant directory for authentication and authorization operations.

- **Which Web technologies does the solution integrate with?**

Due to its open and flexible architecture, Entrust GetAccess has operated with all of the industry leading solutions in the application server, content management, and portal management spaces. Some of the tools that customers have operated with Entrust GetAccess include:

BEA WebLogic	IBM Websphere	ATG Dynamo
Broadvision	Vignette	Epicentric
Plumtree	iPlanet	PeopleSoft
Oracle	Documentum	Others ...

- **Does the solution offer a wireless product today? Can they cite instances where users are accessing online applications and services using PDAs or WAP-enabled cell phones?**

As the use of Web browsers becomes ubiquitous, more and more end users will be looking for the added convenience of accessing their Web services using devices which they carry around with them, eschewing the requirement of being tied to their desktops or even their laptops. Offering these users the access points they need into your infrastructure provides significant opportunities for harvesting and enhancing the relationships you have with them today.

The Entrust GetAccess Mobile Server has been commercially available since Q4 2000. It has been successfully deployed at many customer sites around the world. It is currently being used to facilitate end users registering for services, checking account balances, performing financial transactions, and performing many "traditional" activities without being restricted to their desktops.

5 SUMMARY

When considering a secure Web portal solution, and evaluating the different products available on the market, it is critical to compare capabilities to properly determine which solution will satisfy your needs and help you to succeed in your Web portal initiative.

To best select a Web portal solution, it is imperative to assess the security capabilities of the products you are considering so that your solution offers the level of security to protect your client trust and your company's brand. It is also important that your Web portal solution offers enhanced performance capabilities to allow your infrastructure to scale with the growth of your portal. Finally, you need to evaluate the flexibility of the product to assess whether it can accommodate modifications as your business needs change, and determine whether it is interoperable with the broad suite of technology and infrastructure tools that are needed to successfully operate a Web portal.

This Buyer's Guide has assisted in outlining the various capabilities that Entrust GetAccess enables for your Web portal deployment and how this solution differs from other available solutions on the market. It has outlined the world-class security it offers, the high performance abilities it provides to a Web portal solution and the proven flexibility and interoperability it demonstrates. When comparing solutions in the marketplace to satisfy your Web portal requirements, Entrust GetAccess offers a recognized ability to manage and secure Web access to enterprise applications and services and would be a choice solution to power a Web portal.