Global Information Assurance Certification Paper

Using Portals to Secure Remote Access

SANS Security Essentials
GSEC Practical Assignment
Version 1.4

by Daniel Parker

Contents

Executive Summary

Remote access has moved from a "wish list" item to a corporate mandate over the last couple of years. Two methods have emerged for supplying that access: VPN's and web portals. The word "portal" itself has become a buzzword. For the purpose of this paper, the working definition for "portal" is a hardware and software package used to provide users (inside and outside the trusted network) authentication and access to organizational information. Even this definition may be too broad, as the definition could conceivably be applied to a firewall or any number of web devices. Certainly, these items may be part of a "portal system," but for the purposes of this paper, it is assumed that a portal is a separate set of hardware and software whose sole purpose is to act as the gatekeeper that determines: **Who** is asking for the information? **What** information do they get presented to them? **Where** does that information reside?

Many manufacturers of portals see their offerings as primarily application frameworks, having to do mostly with the graphical user interface. They may or may not recognize the importance of security in their implementations. This paper is intended to address the very important security implications of implementing a web portal.

As stated previously, portals potentially authenticate and authorize users to access information. Certainly these two functions, authentication and authorization, are two key security functions. In the early days of the web, companies put publicly accessible information on the "Internet" and private information on the "Intranet." Anyone who was authenticated to the local area network (LAN) could access the Intranet, and anyone else could access the Internet site. Later, especially as browsers became more standardized, web developers started adding authentication methods to their public web pages, but there were several limitations to these methods. First, the authorization mechanism was fairly monolithic, basically limited to "You're in," or "You're NOT in." Secondly, the Access Control List (ACL) was usually separately maintained on the platform hosting the web site and not connected to any other ACL's already being maintained by the organization (e.g., mainframe ACL's, LAN ACL's, etc.) Thirdly, if information was offered to various classes of external users, such as employees, vendors, and customers, there were usually separately maintained web sites for each group. In other words, there was no "unifying portal" through which these various groups could access corporate information.

Portal technology is aimed at breaking past those limitations. The portal can be linked to the organizational ACL such as NetWare Directory Service (NDS), Microsoft Active Directory (AD), or Security Account Manager (SAM). Next it offers personalization of content since it knows who has logged in. By virtue of these two things, the portal maintains access control throughout the user's visit.

Most importantly, the portal can be given responsibility to add encryption services to the transactions it serves. Placed properly in the architecture of the organization's web infrastructure, the portal can truly help secure the remote user's access to organizational information resources.

Introduction – The Portal as a Security Tool

This paper does not intend to review every portal solution available on the market today. Instead, the author has selected one portal solution that addresses the security features described above. Other solutions may be described to show that more than one solution is available to accomplish the same purpose. The solution that has been selected for this paper is Stoneware's B2B Web Portal.

According to a November 2001 CIO white paper[1], it is noted that a portal should provide "security (your systems and content are accessed only by those who are supposed to access them)." The document goes on to describe the following areas in which a portal solution provides security:[2]

- Authentication
- Authorization
- Logon
- Single sign-on
- User management
- Digital certificates
- Public key
- Digital signatures
- Public key infrastructure (PKI)
- Secure socket layer protocol (SSL)
- Secure hypertext transfer protocol (https)

While some of these areas may be addressed by existing infrastructure, the portal solution itself will either tie into these security issues by reference, or be supplied directly by the portal itself. Later, this document will show specifically how these areas are addressed in Stoneware's portal solution.

[1] Author Unknown, "Understanding Portals: A Business Person's Guide to Enterprise Portal Terms and Business Impacts," November 2001, URL: http://www.cio.com/sponsors/portalswhitepaper.pdf, page 3.

[2] Ibid, pp. 18-22.

Portal Features

What is a portal? In Unitas' white paper, "Enterprise Information Portals: What They Are, Why They're Important, and Why You May Need One", several business challenges are outlined that are the target of the portal industry[3]:

- Too much fragmented structured and unstructured information – valuable company information exists in different formats, residing in many repositories and locations throughout the organization that employees either do not know exist or cannot access to do their jobs
- The inability to realize the return on the substantial investment in information systems and reduce the cost of operations. Organizations are constantly replacing or enhancing information systems
- The inability to improve employee productivity and produce greater results with limited personnel resources
- The inability of employees to collaborate and share valuable information both within and without the enterprise to make faster and better informed decisions, as well as to drive out process inefficiencies both internal and external to the enterprise
- The lack of flexibility, time to market and competitive advantage due to the fragmented and nonintegrated information and systems to support the dynamic change in the market and business
- Major companies are under increased pressure to collaborate, build tighter relationships and share information among employees, customers, suppliers and partners and make faster and more informed decisions.

With these challenges in mind, portals must deliver the means to do the following: authorize access, authenticate users, provide a means to personalize content, and secure the information presented against unauthorized access, defacement, and a whole host of other threats.

Authenticating and Authorizing Users

Authentication establishes **who** you are before you are given access and *authorization* establishes **what** you can access. The two terms are not synonymous. Perhaps the portal contains software that establishes who is logging in, but might rely on legacy systems that actually contain the data to supply the access controls. Here, one sees how integral the issue of *user management* is to the discussion. Such a decentralized scenario would be in regard to user maintenance. A separate user account would need to be managed on each system accessed. This also points out how important *single sign-on* might be to an

---

[3] Staff Writer, Unitas Corporation, "Enterprise Information Portals: What They Are, Why They're Important, and Why You May Need One", March, 2001, URL: http://www.portalscommunity.com/content/display/BB0F160C-267A-42DF-A15A8059D92BC4BE.pdf, pp. 4-5.

organization so that a user would not be burdened with supplying a separate username and password on each system they have access to.

Personalized Content

Portal technology has long focused on the delivery of personalized content. Corporate information is typically stored on several different platforms in various locations. Different people are interested in different information. Presenting a user with a menu listing all information available in all locations would be cumbersome at the very least. And offering on that menu information that you intend to withhold due to access controls would be impolite at best and a security breach at worst. The best situation would be to show only the items you intend to offer access to.

Data Security and Integrity

The organization has a great interest in making sure that sensitive information is not compromised as a by-product of being offered over the Internet. Sending information in clear text may not be desirable. If users are allowed to contribute content during their portal connection, the organization may need to guarantee the identity of the contributor by means other than just a login with a password. In e-commerce transactions, non-repudiation is obviously a goal. As the CIO white paper explained, "Using the HTTPS protocol will inspire confidence in your users that the information being passed is secure."[4] In addition to HTTPS, other protocols such as PKI, SSL, and digital signatures and/or certificates can be used for similar purposes.

Portals can help to further isolate web servers from the public Internet. This translates into further protecting web content from possible attacks such as vandalism.

Portals and The Directory

In a presentation prepared for The Meta Group, David Folger recognized the importance of security. He states, "Employee portal focuses on authentication and authorization; Internet access of portal introduces the need for encrypted data and published security/privacy statements." He goes on to add, "Directory integration is a critical need for employee portals."[5] His comments may well be extended to other types of portals other than just employee portals.

---

[4] Author Unknown, "Understanding Portals: A Business Person's Guide to Enterprise Portal Terms and Business Impacts," November 2001, URL: http://www.cio.com/sponsors/portalswhitepaper.pdf, page 22.

[5] Folger, David, "Corporate Portals: Trends and Architectures", URL: http://www.intraware.com/bindocs/portalserver/portals_folger.pdf, page 10.

Types of Portals

By Target Audience

One way to classify portals is by the audience using the portal. The portal industry has used the B2* (short for Business-to-*) title to enumerate these classes. B2E is the classification given to Employee portals. This was perhaps the first entry point for many organizations into the portal market. Organizations were looking for ways to organize data for presentation to employees using a common interface such as a browser. This may have begun as an Intranet project, but soon there was a recognition that employees may need this access from home, or from remote locations in addition to being able to gain access from their office desks.

The Business-to-Business (B2B) portal is another obvious portal application. Similar to the Intranet-B2E link stated above, the Extranet may have been the genesis of the B2B portal application. There are obvious security implications that are a little more complex than the B2E implementation. Organizations are quite a bit more nervous granting access to people outside the organization than inside. Secure communications are required between organizations to establish usernames and passwords. Consequently, user maintenance is more problematic.

Last but not least would be the Business-to-Customer (B2C) portal implementation. The first obvious difference between this portal application and the others is the scale. An organization may have hundreds of employees, thousands of vendors, stockholders and other B2B relationships and millions of potential customers. User maintenance is a whole new ballgame in this arena. It might include self-registration as one of the requirements of a portal solution.

By Function

David Folger listed four functional categories for portals: decision, collaborative, publishing and operational portals.[6] The decision portal obviously supports the decision-making process inside or between organizations. The decision portal was briefly described by Randy Frid, PhD., Principal Scientist, and Randall Eckel, President and CEO of the portal vendor, InfoImage.

> Decision portals fundamentally change the way knowledge workers approach decision-making processes. Their tangible benefit is to speed the information gathering and collaboration processes so that knowledge workers can bring significantly more information and experience to bear, as well as spend more time in the "decision" step of the process. Decision portals provide the technology to truly decentralize and optimize the

[6] Folger, page 6.

> decision-making process throughout an enterprise and the extended enterprise.[7]

The collaborative portal focuses on the need for individuals to collaborate in the design, writing and production of various types of information. An example of a collaboration portal is the Brava! Central Portal. (See http://www.bravacentral.com/main.htm) As far as its security features, the vendor's product sheet states,

> "Security? No problem. Information sent over the Web is in a compressed display format viewable only by authorized users. So, documents and drawings are never at risk of being copied or stolen. Brava! WebKit also operates seamlessly with existing firewalls and encryption tools without requiring any adjustments or additional software."[8]

The publishing portal simply publishes documents in a highly organized manner to facilitate the portal user's ability to find documents quickly and securely. With respect to operational portals, the author of this paper was not able to find any portal describing itself to be an "operational portal." A further hint about the nature of operational portals may have been given in a quote from David Folger himself. Business Wire quoted him as saying,

> "As the market matures, enterprise portals will integrate operational applications with other functions such as knowledge management, collaboration, business intelligence solutions and other transactional systems," said David Folger of the META Group. "PeopleSoft's portal addresses these other functions as well as providing a portal interface to its own applications."[9]

Thus, it could be assumed that operational portals deliver operational applications. This might include B2C portals that deliver e-commerce applications, B2E portals that deliver information about the employee's 401K portfolio, etc.

---

[7] Frid, Randy, and Eckel, Randall, "Streamlining the Decision Cycle Through Collaborative Decision Management**",** May 2001, URL: http://www.kmworld.com/publications/whitepapers/ECM/frid&eckel.htm, page 3.

[8] Product Sheet, "Brava! Central, Collaborative Document Portals", Informative Graphics, URL: http://www.bravacentral.com/pdf/BravaCentralBrochure.pdf, page 3.

[9] StreamingMedia, Business Wire, "Peoplesoft Unveils Portal Solutions; Portals to Deliver Role-Based Content to Customers, Employees, And Suppliers," October 2, 2000, URL: http://industry.java.sun.com/javanews/stories/story2/0,1072,30189,00.html

A Real-World Example

Why Stoneware?

There are many manufacturers of portal solutions. The portal solution by Stoneware, Inc. was selected for this paper for its unique combination of security features. Although Stoneware incorporates many security features, one of the most unique features is its "relay" architecture, which will be more fully explained later in this document. In the company's main white paper, they state, "Stoneware's relay architecture makes it one of the most unique and secure portals in the industry."[10] Many of Stoneware's other features are perhaps less unique.

Few of the other portal solutions reviewed by the author stressed security as much as Stoneware in their corporate literature. That is not to say that other manufacturers do not place importance on their security features. Notice the placement of security in Hummingbird's statement found in their white paper describing their portal solution: "The most critical of the principal elements are: security, presentation, personalization, collaboration, publishing and distribution, integration, interactivity, categorization, search, multi-repository support, and metadata management."[11] Netegrity claims to be "the leading provider of software solutions for securely managing e-business."[12] In the past, they combined their SiteMinder software with portals such as Plumtree's to add security features such as directory integration and single sign-on. Although they continue to do this, the company recently introduced their own full-featured portal solution, calling it Netegrity Interaction Server. Where SiteMinder provides a single sign-on doorway to various other authorization mechanisms, Interaction Server provides deeper security integration.[13]

In an article about Netegrity's Interaction Server, one analyst was quoted as saying, " 'The portal is the one place that security has to happen,' says Larry Hawes, senior advisor

---

[10] Stoneware, Inc., "Stoneware White Paper," URL: http://www.stoneware.com/whitepaper.pdf, page 5.

[11] Hummingbird Corporation, "Enterprise Information Portals: Meeting the Needs of Technology and Business," URL: http://www.hummingbird.com/collateral/eipmeetingneeds_whitepaper_EN.pdf page 5.

[12] Netegrity and Plumtree, "Integrating Netegrity SiteMinder with the Plumtree Corporate Portal." URL: http://members.netegrity.com/access/files/Plumtree_Netegrity_Joint_White_Paper.pdf, page 10.

[13] Mears, Jennifer, "Netegrity Pushes Into Portals," NetworkWorldFusion News, March 25, 2002, URL: http://www.nwfusion.com/news/2002/0325netegrity.html

at The Delphi Group. 'If you're using the portal to aggregate information sources and back end transactional applications you want to make sure you're regulating pretty tightly who can access those, especially when access is available not only to employees, but to partners, suppliers and customers.' "[14]

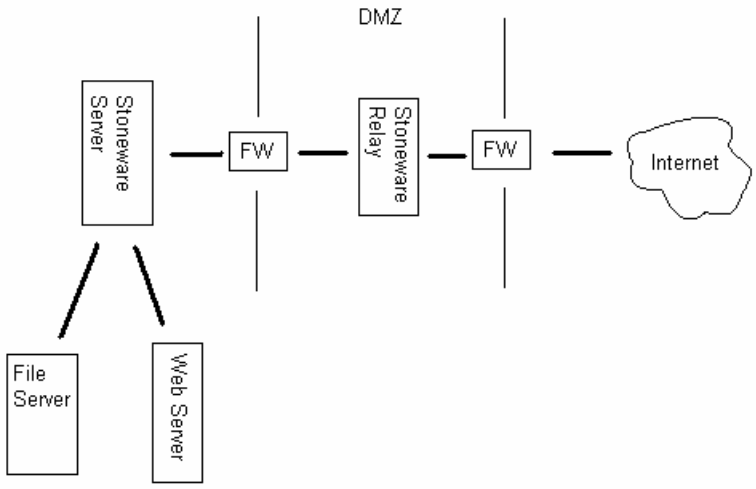
Stoneware appears to fully understand this concept. They have tightly integrated their product with Microsoft's Active Directory (AD) and Novell's NetWare Directory Service (NDS). Stoneware plans to support other LDAP-based directories in the near future. This integration provides the tight regulation of who accesses what as stated above. In addition, other Stoneware features such integration with SSL and their unique relay architecture further protect the privacy of transactions through the portal. These two components provide for all of the areas of security mentioned in the first section of this paper. The following table shows how these two components address each issue.

Security Issue	**Directory Integration**	**Relay Architecture**
Authentication	Handled by DS	
Authorization	Handled by DS	
Logon	Handled by DS	
Single sign-on	Passwords stored as user attributes	
User management	Handled by DS	
Digital certificates		Proxied by Relay
Public key		Proxied by Relay
Digital signatures	Can be managed by user by DS	Proxied by Relay
Public key infrastructure (PKI)		Proxied by Relay
Secure socket layer protocol (SSL)		Proxied by Relay
Secure hypertext transfer protocol (https)		Proxied by Relay

Stoneware Architecture

The following diagram illustrates the basic architecture of the Stoneware Portal.

[14] Ibid.



The above diagram shows two separate physical components: the Stoneware Server (also referred to as the Stoneware Loader in some of Stoneware's literature) and the Stoneware Relay. Both components can be installed on one of the following platforms: Novell NetWare, Microsoft Windows NT/2000, or Linux. Directory Services must be either Novell's NDS/eDirectory (which runs on all of the platforms listed) or Active Directory (which runs only on Windows 2000). The owner of Stoneware Portal may operate an unlimited number of relays with each licensed Stoneware Server. This provides load balancing and redundancy. On the other hand, it is possible (though less desirable from a security standpoint) to run both the server and relay components on a single server.

(Note: Much of the following information was obtained from a manual produced for the Advanced Stoneware Training Course periodically offered by Stoneware, Inc.)[15]

Stoneware Server (a.k.a. Stoneware Loader)

The Stoneware Server component provides the following functions, directory access, session management, access control, and data access.

Directory Access

The Stoneware Server provides access to the directory in one of two ways. First with either AD or NDS, the server uses Lightweight Directory Access Protocol (LDAP). This connection can be a secure one in which directory information is encrypted between the server and the directory. Another handy feature of the LDAP connection is that the server will automatically attempt a reconnection with the directory should the connection become broken for any reason. The second way in which the server can connect with the directory is Novell's Java Client Libraries (NJCL). NJCL is, of course, only available when using Novell's eDirectory. This option establishes a direct DS connection and does offer the reconnection feature offered by LDAP.

[15] Stoneware, Inc., "Stoneware Advanced Training," April 23, 2002

Session Management
As soon as a user authenticates to directory services a session is established between the user's browser and the Stoneware Server. This session cookie is sent to the browser. The cookie maintained by the server manages information such as the user's access control rights, his credentials, and personalization information. This cookie is maintained until either the session times out due to inactivity, the user logs out or closes his browser, or the server is restarted. Since the connection is maintained between the Stoneware Server and the user's browser, the user can switch between multiple relays during the session without having to re-login.

Access Control
The Stoneware Server caches the user's access control list (ACL). Thus, when a user requests a service for which he is not authorized, the Server directs the relay not to service the request. Since the personalization features see to it that the user is not presented with components to which he doesn't have access, this denial of a request is less likely to happen. Again, since the ACL is cached at the server, it doesn't matter which relay the user comes through. His rights are the same no matter which relay he hits.

Data Access
Using various methods, including Simple Object Access Protocol (SOAP) and various Stoneware API's, the Stoneware Server can gain access to various data sources. These sources include the directory service itself, ODBC databases such as Access, MySQL and many others, and to XML documents.

Stoneware Relay

The relay establishes its communication with the Stoneware Server with the Java protocol called Remote Method Invocation (RMI). The default port for RMI is 1099. Once that connection is established the server and the relay negotiate a high port over which they continue the rest of the conversation. All port numbers used can be configured by way of a configuration file. The high port used can be configured to be dynamic or static. The configuration can also handle situations in which the relay and the server are separated by a NAT.

As stated above, the server always determines what the user has access to. If the user has access to a HTTP or HTTPS device behind the internal firewall, the relay can establish a direct connection to that device. In this case, the relay acts as a proxy in that the user is establishing a direct connection with the HTTP/HTTPS device, but the relay is establishing a connection on behalf of the user. This connection is defined in what is called a "Stoneware Map." Stoneware Maps can be configured to utilize an internal (i.e., behind the "inside" wall of the DMZ) proxy server. If there were multiple HTTP/HTTPS

devices to be mapped, using an internal proxy would simplify the configuration of the internal firewall.[16]

Very similar to the Stoneware Map, there is another directory object called the Stoneware Port Map. The only difference is that the Port Map can communicate with any TCP/IP device such as an FTP server, a Telnet server, a VNC host or a terminal server. As in the case of the HTTP device connection, the Stoneware Server must first determine if the user has access rights to the TCP device defined by the Stoneware Port Map. Once that is determined, the Stoneware Relay establishes a direct connection with the device on behalf of the user. Other characteristics differentiate Stoneware Maps from Port Maps. Data passed via a Stoneware Map can be SSL-ized by the Relay. Stoneware Port Maps rely on the protocol being relayed for encryption (e.g., VNC, SSH, etc.). Similarly, Maps support internal proxies; Port Maps do not.

Stoneware and SSL

The importance of SSL is evident as it is the first of 21 features listed in their main white paper. According to the document, "Stoneware provides SSL (secure socket layer) services to all web resources located behind the Stoneware web portal. All web servers and application content accessed through the web portal will be encrypted through SSL with a single certificate."[17]

Some critics have attacked SSL as being over-sold and somewhat insecure. (See "SSL Leaves Gaps for Hackers – Are Web Sites as Secure as They Seem?" http://www.securitynewsportal.com/cgi-bin/cgi-script/csNews/csNews.cgi?command=viewone&id=74&database=JanK%2edb.) One company, ArticSoft, calls SSL "a condom that is open at both ends." They complain, "My data is SSL protected between the server and me, so why should I worry? Well, no one at the server end really knows who the data is from because they don't know what your identity is. They assume that data arriving through the pipe is right, and that your identity can be presumed from the data, not the other way around."[18]

Stoneware supplies the identification of the user at the one end by using the directory service to authenticate the user's credentials. Usually this means username and password, but could potentially use whatever means the directory service supports, such as biometrics, certificates, smart cards, etc. A known and publicly verified certificate

---

[16] Stoneware, Inc., "Stoneware Advanced Training," April 23, 2002, p. 8.

[17] Stoneware, Inc., "Stoneware White Paper," URL: http://www.stone-ware.com/whitepaper.pdf
page 2.

[18] ArticSoft, Limited, "Does SSL Protect You, Or Is It a Condom That Is Open at Both Ends?" April 30, 2002, URL: http://www.articsoft.com/wp_ssl_condom.htm.

(e.g., Verisign, Thawte, Entrust, etc.) at the server end can help assure the user that the server end is who he says he is.

Conclusion

By using a Stoneware Web Portal, an organization can provide its employees, suppliers, stockholders, customers and other stakeholders secure access to information resources. Those resources that may have previously been located inside a firewall DMZ can now be placed all the way *inside* the interior wall of the DMZ. The entire transaction including the authentication itself can be encrypted from remote user to the internal resource.

List of References

ArticSoft, Limited, "Does SSL Protect You, Or Is It a Condom That Is Open at Both Ends?" April 30, 2002, URL: http://www.articsoft.com/wp_ssl_condom.htm

Author Unknown, "Understanding Portals: A Business Person's Guide to Enterprise Portal Terms and Business Impacts," November 2001, URL: http://www.cio.com/sponsors/portalswhitepaper.pdf

Folger, David, "Corporate Portals: Trends and Architectures", URL: http://www.intraware.com/bindocs/portalserver/portals_folger.pdf

Frid, Randy, and Eckel, Randall, "Streamlining the Decision Cycle Through Collaborative Decision Management**",** May 2001, URL: http://www.kmworld.com/publications/whitepapers/ECM/frid&eckel.htm

Hummingbird Corporation, "Enterprise Information Portals: Meeting the Needs of Technology and Business," URL: http://www.hummingbird.com/collateral/eipmeetingneeds_whitepaper_EN.pdf

Mears, Jennifer, "Netegrity Pushes Into Portals," NetworkWorldFusion News, March 25, 2002, URL: http://www.nwfusion.com/news/2002/0325netegrity.html

Netegrity and Plumtree, "Integrating Netegrity SiteMinder with the Plumtree Corporate Portal." URL: http://members.netegrity.com/access/files/Plumtree_Netegrity_Joint_White_Paper.pdf

Product Sheet, "Brava! Central, Collaborative Document Portals", Informative Graphics, URL: http://www.bravacentral.com/pdf/BravaCentralBrochure.pdf

Staff Writer, Unitas Corporation, "Enterprise Information Portals: What They Are, Why They're Important, and Why You May Need One", March, 2001, URL: http://www.portalscommunity.com/content/display/BB0F160C-267A-42DF-A15A8059D92BC4BE.pdf

Stoneware, Inc., "Stoneware Advanced Training," April 23, 2002

Stoneware, Inc., "Stoneware White Paper," URL: http://www.stone-ware.com/whitepaper.pdf

StreamingMedia, Business Wire, "Peoplesoft Unveils Portal Solutions; Portals to Deliver Role-Based Content to Customers, Employees, And Suppliers," October 2, 2000, URL: http://industry.java.sun.com/javanews/stories/story2/0,1072,30189,00.html