A BIO-key® Solution.

White Paper

Designing and Implementing A Secure, Fully Brandable Web Portal

Table of Contents

Summary

What is a Portal?

In simple web terms, a portal is a website that provides users with access to information from various sources in a single location. A portal acts as a gateway that brings the individual and required resources together with minimal external travel necessary.

In recent years, however, the notion of a portal has taken a more dedicated turn. The question is no longer 'what is a portal' but rather a combination of, 'how secure is it,' and, 'what can it do for me?' With various industries and departments requiring their own version of a web portal, simply knowing the definition is only a small fraction of understanding the true benefits of a portal. Making an informed decision is an integral step towards providing the best experience for your digital environment.

Four Major Types

Web portals come in various guises – sometimes it can be very difficult to understand which type of portal is right for you. To put it simply, web portals can be categorized into four major categories, as follows:

Enterprise

An Enterprise Portal is a centrally administered framework that provides information and access to data, tools, and programs owned or specifically required by a company or organization. Oftentimes, Enterprise Portals combine personal and company-related data together in a private and secure environment.

Security: Access control, auditing, SSL encryption, ACL Management.

Web

A Web Portal is a public point of access that aggregates content such as news and weather alongside personally customizable features; i.e. e-mail, social media feeds and updates. This information is hosted on the web, and the portal is typically accessed through any web browser.

Security: Various, depending on integration. SSL encryption is typical, along with some Multi-Factor support.

Captive

A Captive Portal is a public-facing web page that is presented to the user before granting access to the Internet. Typically, Captive Portals require specific credentials before Internet access is granted. A popular example of a Captive Portal is the web page displayed to guests at most major hotels before access to local Wi-Fi is granted.

Security: Key-based Wireless Network encryption (WEP/WPA keys are typical), end-to-end data security, ACL management.

Intranet

An Intranet Portal is similar to an enterprise portal in that it offers access to enterprise specific information, applications and managed content. The primary difference between an Intranet Portal and an Enterprise Portal is that an Intranet Portal may only access resources that are hosted/located directly within the enterprise environment, without accessing the external Internet.

Security: Access control, auditing, content verification, SSL encryption, ACL Management.

Portal Functionality

Typical Features

With the notable exception of the Captive Portal, each major type of web portal focuses on varying forms of the same thing: providing end-users with relevant information. The information that is required, and therefore displayed, varies based on what information is already available to the client via intranet access, and which applications can be redirected to from within the portal itself

According to an online survey of CMS portals published by Purch , most feature sets center primarily around the following five categories:

Content Management	Information Library	Project Management	Direct Communication	External Integration
• Photo Galleries • File Sharing • Featured Content • Wiki/FAQs • Surveys/Quizzes	• Search Engine API • Forums • Mailing Lists	• Newsfeed • Event Planning • Calendar • Contacts	• Chat/IM • E-mail • Announcements	• eCommerce • Maps • Weather

Interestingly enough, security features and the applications themselves tend to take a backseat in most web portals, with priorities being centered mostly on announcements, content management, and direct information access behind a single username and password. As noted above, most security features native to typical portal software are limited to the basic essentials: Firewall/ACL control, Access Control, SSL encryption, and auditing. In the end, the environment in which the portal is integrated determines the true security of a portal.

However, with each year bringing about an increasing amount of drastic data breaches and cyber attacks, adequate security has become more of a necessary feature in modern portals. In this climate, a new take on the web portal needs to pick up the slack.

A Seamless Integrated Secure Portal

As noted, portals by their very nature are a great way to collect, collate and present data to the end user. The modern web portal needs to address the delicate balance between security and usability to provide the best user experience possible. There is no doubt that the end user experience is a primary driver in selecting and designing the right type of portal, but reaching that goal requires the consideration of numerous additional factors.

Security, compliance, design and integration all come to mind when considering how to create an exceptional user experience. The perfect portal will meet all of your needs with one solution, without requiring you to bring in additional pieces to fill in the gaps.

"Security should never be an afterthought when integrating a portal into your environment"

Security Considerations

Addressing security considerations with a portal alone need not be a monumental task. Access control, ACL management, and content verification are the first steps in providing a secure portal for your environment, but security considerations encompass a much wider array of access – after all, sensitive data can mean web content, applications access or even downloads. To produce a portal that provides exactly the right type of security that your environment requires, without missing a beat, certain questions need to be asked:

Some questions to consider:

- Will you be using a User Repository for access control?
- Do you require access from within a corporate network or without? What about both?
- How will credentials be verified?
- Will the portal act as an IdP?

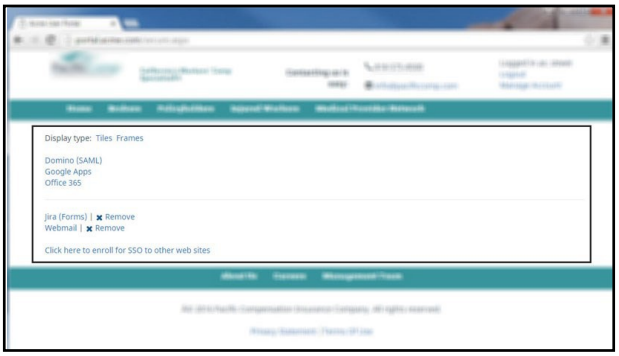
The biggest question to ask yourself straight off the bat is this: What security features do I need? Security should never be an afterthought when integrating a portal into your environment.

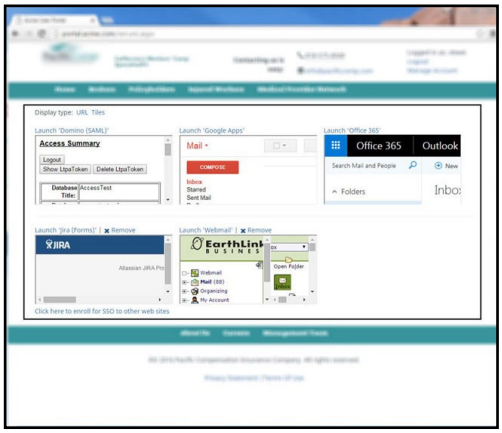
The type of user repository that you use may limit your choice for a fully integrated portal, while necessary external access may also trim your available options. It then becomes a question of whether or not your environment can make certain sacrifices for the sake of user convenience, when in reality you may not need to.

In terms of securing sensitive data, your portal should be a place where the worlds of the public portal and private portal collide into a single, seamless experience. Private information should never be accessible in the same way that public information is provided to users – and the use of multiple login portals can prove to increase user frustration rather than decrease it.

When securing sensitive data, a new series of questions need to be considered, specifically focused on how access to that data will be granted. If your main goal is to improve user experience, streamlining application access is a major factor. A top consideration for this security measure is the use of industry standard protocols.

For example, the use of SAML for Single Sign-On - or the equivalent - would help thread the needle between security and usability for application access. Other methods of access to consider when SAML is not available are Forms-based, or possibly even Kerberos authentication for local web applications.





Examples of SSO Integration

Designing a portal with Single Sign-On capabilities offers administrators and users alike a great many benefits. Having a central access point to web apps allows users the convenience of maximizing their portal experience and efficiency. There are a number of ways to allow this integration, whether it is done through a jump page, icon tray, frames or links. Each has advantages and disadvantages and understanding those is a key consideration.

Of course, there are many security related questions that present themselves when it comes to securing sensitive data alongside publicly available content, and each organization will have to carefully consider them based on their own merits. The underlying takeaway is that providing secure access does not necessarily need to become an obstacle in providing the optimal portal experience. Addressing these questions initially will allow you to avoid issues in compliance, design and integration considerations as well.

Compliance Considerations

Regardless of your industry, security requirements feed directly into compliance considerations. The two are often treated as one in the same, as they rely so heavily on one another. Whether you are dealing with internal corporate policies or federal compliance standards such as HIPAA, FERPA or COPPA – or even PCI Compliance – these standards will have a major influence on the design and overall implementation of your integrated portal.

Some questions to consider:

- Will the portal address internal policy requirements?
  - Password management, complexity, expiration, etc.
- Is there a full range of auditing capabilities built into the software to track portal access records?
  - Successful/Failed attempts, typical time of access, etc.
- Will File Sharing (a typical feature of a CMS portal) put sensitive, private data at risk for external exposure?
- Is the portal compatible with Multifactor Authentication?

Compliance standards can make or break the installation of a new software solution, often even more so than user adoption. Addressing these concerns in the early stages of product evaluation ensures that more issues do not need resolving down the line.

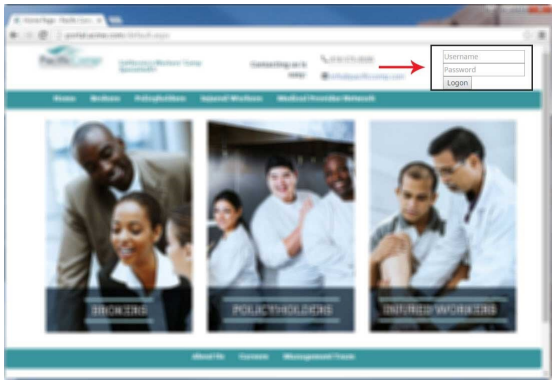
Portal Integration Points

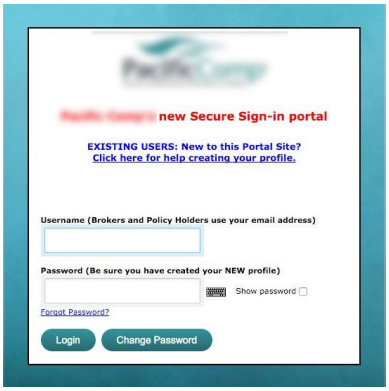
Understanding and addressing security and compliance requirements is all well and good, but the design and integration points that your new portal implements are of vital importance as well. Even if the software meets all other requirements, the functionality of the portal will go a long way to determine whether or not users will still be willing and able to make appropriate use of it.

Some questions to consider:

- Do you want a fully integrated login form on an existing page, or a separate login page for access to the portal?
- Will announcements be targeted to specific users based on user repository organization?
  - AD Users/Groups, etc.

- Will access be provided to all required applications based on the strength of the portal login or will additional credentials need to be provided for every login?
- Does the branding match that of the rest of your website?
- Can you customize error messages to provide useful information for end users to learn from?





Examples of each distinct integration method

Each of these questions addresses a factor that ultimately leads to the user experience surrounding your new portal; too much functionality can be overwhelming and reduce productivity, while not enough can produce more work that is required, or even turn your end users away in frustration.

Integration is all about bringing everything that a user may need without the extra hassle and an appropriate portal installation must keep this in mind. Not only does the portal need to integrate well with your existing website, software and applications, but it must also integrate with the multitude of needs surrounding appropriate implementation and end user experience.

End-user Considerations

One of the most important integration points to consider is the location of the login itself. Brandability and customization are huge benefits that not only improve the usability of the website, but also provide end users with a consistent look and feel while navigating through familiar territory. Flexibility to adjust the location of the login screen and streamline access can help take some of the frustration out of the necessary security and compliance related measures as well.

While concerns in the realm of security and compliance are important, the UI and content elements of a portal often get the lion's share of attention - as they should. A well-received and useful portal relies on its ability to deliver pertinent information in an efficient and accessible manner. Things like branding, color schema, and fonts serve to convey a reassuring message of corporate consistency and engender trust on the user's behalf that they are in fact on a company-sanctioned site.

When considering the user experience it's always a good idea to "walk-the-journey" with them. After all, users are going to have questions of their own.

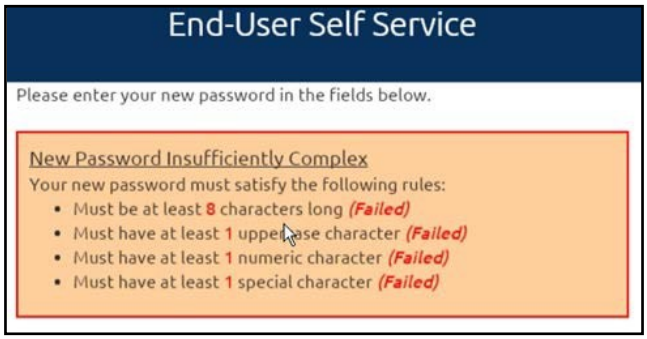
Questions like:

- Where do I login?
- What happens once I login?
- How do I enroll my phone?
- Do I need to sign into my e-mail after I login here?

The integration considerations and design elements can be a huge step towards addressing these potential user considerations. Subtle design elements can often make a big difference in how well a portal is received. For example, when the user logs in, are they able to access a wide variety of their web based applications via a single click or do they have to constantly login to each application they choose to interact with? As we noted before, convenience and usability do not need to be a drain on important features such as security capabilities.

Additional considerations like meaningful error messages when a user fails to login, or clear, relevant information on how to reset a password also lend greatly to the overall end user experience.

When everything is all said and done, your final goal is a fully functional portal that meets the specific requirements of your environment while appealing to the users who will be spending every day using it. It's a complicated line to walk, but one that doesn't need to be hard to manage.



Technical Consideration

Last, but certainly not least, are the various technical considerations that go into implementing and servicing a new portal. If everything else has been designed, analyzed, etc., the technical aspects still need to bring everything together into a cohesive whole.

Having a well-designed and highly secure portal are certainly the primary goals of any I/T implementation but there are many "behind-the-scenes" elements that also need to be considered:

Questions to consider:

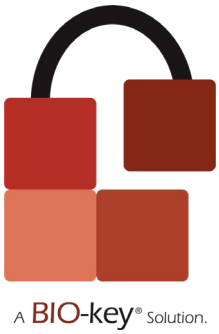
- Will you host this portal on-premises or in the cloud?
- Does the portal come with failover protection in case of server outages?
- How does the portal handle traffic spikes?
- Is there out-of-the-box load balancing support?
- How will you host this portal?

It is unwise to assume anything in terms of appropriate software integration, and making sacrifices at this stage can lead to spending more money down the road, and a whole host of unnecessary frustration on both the end-user and administration side of things. If a portal implementation is going to be successful, it needs to be fully fleshed out from design, to implementation, all the way through to the back end.

Conclusion

The digital marketplace is a continually evolving community of applications and services that exist to improve every facet of life for the end-user. The end-user can be either the individual using a service that an organization has put into place, or the administrator working towards implementing the perfect solution for his or her environment. Everyone has their own set of needs, and the perfect solution must be up to the challenge of meeting those needs, as they arise – not after the fact.

Typical web portals provide a variety of options aimed primarily at convenience – and convenience is great, but security should never be reduced to an afterthought. With the evolution of the digital environment that we each traverse every day, there's no reason to settle for simple convenience when your portal can also be packaged with strong security in the same package. Things are constantly changing – your portal should never be left behind



About Us

BIO-key International is an innovative provider of access management and biometric identity solutions that enables convenient and secure access to devices, information, applications, and high-value transactions. BIO-key offers the simplicity and flexibility required to secure the modern digital experience for the workforce, customers, and IT department.

BIO-key's PortalGuard is a complete Identity & Access Management (IAM) platform with industry-leading biometric identity options for single sign-on, multi-factor authentication, adaptive authentication, and self-service password reset.

Backed by decades of expertise, BIO-key has a proven track record of successful IAM project delivery, strong customer relationships, and low TCO.

Visit www.BIO-key.com for more information.