

Quick, cost effective and secure control of Microsoft SharePoint for internal and external user communities with granular access controls

OVERVIEW

SharePoint is Microsoft's fastest growing enterprise solution in company history, with over 100 million licenses, \$1 billion plus in revenue and growing. Organizations that choose SharePoint to enable collaboration across user communities are experiencing an explosion in the number of sites and are battling the complexities associated with managing users, their association with SharePoint permissions and enforcing enterprise security policies. As SharePoint instances spawn at an impressive rate, the challenge of protecting sensitive corporate data while fueling collaboration grows and the native capabilities within SharePoint are proving insufficient.

BiTKOO has developed a solution to enhance the built-in authentication and authorization capabilities within SharePoint, consisting of two main components.

The first deals with externalizing SharePoint instances to authorized B2E and B2B users. SecureWithin™ allows organizations to expose SharePoint instances to external clients, quickly and cost effectively without VPN, DMZ replication




or network and firewall reconfigurations. The second deals with the static controls in SharePoint, the proliferation of permissions in an enterprise deployment and the limited ability to plug into an identity centric access control model. Keystone™ provides fine-grained access control for consistent, dynamic authorization management across SharePoint instances and organizational boundaries for complete control and audit of user entitlements. SecureWithin and Keystone work seamlessly together or can be deployed separately depending on requirements. The solution is designed to leave alone the document specific controls, i.e. the things SharePoint was designed to manage (Full Control, Design, Contribute, Read, Limited Access, etc.) and associating those controls to users, roles and any number of sources to collectively determine who has access to what and who can perform what function.






THE CHALLENGE

Organizations are discovering inherent weaknesses in the SharePoint security model as the tool moves from a tactical solution to an enterprise one. Access control in SharePoint becomes critical as servers take on more and more confidential company data. There is no

DIRECTORY ABSTRACTION

-  Consume authentication from any provider (not just AD)
-  Consult any number of authorization sources
-  Make authorization calls out to legacy systems

EXTERNALIZE AUTHORIZATION

-  Apply consistent fine-grained controls
-  Call out to any legacy system
-  Run-time decisions for dynamic controls

FULL AUDIT TRAIL

-  Snapshots of SharePoint access across all sites
-  All user and administrative activities
-  Complete transparency into SharePoint and across the application environment

SHAREPOINT SECURITY WITHIN MINUTES

KEY BENEFITS

Active segregation of duties enforcement

Enterprise Authorization Management

Delegated administration w/fine-grained controls

Rich context and conditional expression

Role & Rule Management

synchronization with Active Directory and SharePoint maintains groups and permissions in its own database. SharePoint does not easily integrate with Identity sources and the need to do so is obvious as SharePoint becomes an enterprise level application.

According to Gerry Gebel, VP and Services Director for the Burton Group's Identity and Privacy Group, "Everything would be fine if you were not trying to hook up SharePoint with your identity management tools. SharePoint is going to be a critical application and granular access controls will be a necessity and Microsoft's tools are insufficient for all usage scenarios."

Other issues include the need to manually map users or groups to permissions. Because SharePoint has many levels where permissions can be set (List, Site, Level, Personal) the sheer number of pre-established permissions becomes unmanageable. Add to this the need to manage enterprise policies across SharePoint and the rest of the application infrastructure and the cost and complexities grow by orders of magnitude.

THE SOLUTION

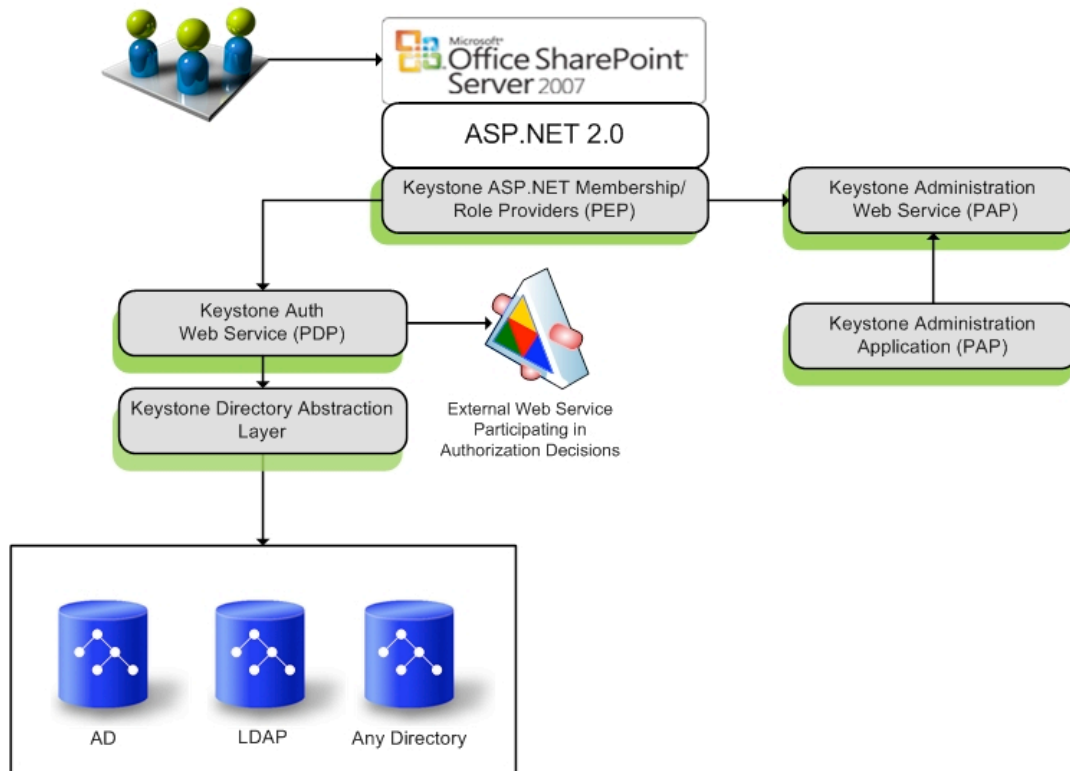
Keystone is an engine that provides the authentication and authorization services for applications and web services security. The product is comprised of a set of web services, administration applications, databases and application-side, framework-specific components. The main aspects of Keystone consist of authentication abstraction and fine-grained authorization.

The authentication abstraction aspect means that Keystone can connect to any number of authentication providers, such as LDAP, Active Directory, RADIUS, etc. It then provides an abstraction layer above these existing

authentication providers. When SharePoint needs to consume a new kind of authentication, or when the underlying authentication provider needs to be replaced, SharePoint does not need to be modified because it consumes authentication from the abstracted Keystone layer and not from the authentication source(s) directly.

Keystone provides fine-grained authorization for SharePoint through run-time calls to any number of authorization sources containing user attributes. Keystone determines what role a user has, and that role is then allowed group access in SharePoint with their associated permissions. Keystone-enabled SharePoint enjoys a stable, immutable security-related lifecycle because enterprise policy, identity management and role management are determined outside of SharePoint and bring these authorization factors into the SharePoint access control equation.

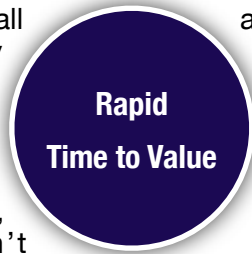
Keystone runs on any device and is supported across all major platforms. SharePoint runs on ASP.NET 2.0; Keystone for SharePoint consists of two DLLs that need to be registered with ASP.NET for the SharePoint instance. Keystone allows SharePoint to leverage authorization decisions based on either static or dynamic assignments of enterprise or application specific roles based on run-time queries for attributes in any number of systems. Delegated administration, segregation of duties and complete audit trail and reporting are now available across SharePoint and any number of other Keystone enabled applications. Keystone comes with an import tool that allows organizations to effortlessly convert all existing authentication and authorization attributes from SharePoint into Keystone so that



Keystone works in tandem with native SharePoint permissions

there is no need for manual conversion. The solution has a feature called Directory Sync which keeps SharePoint user attributes in sync with those from the originating directory or other user store.

SecureWithin is a complementary product to Keystone and it provides SharePoint a secure tunnel accessible to authorized clients on the Internet. Federated authentication and cross-firewall access between SAML-enabled identity providers is handled with ease. In addition, for clients not employing SAML, Single Sign On (SSO) is facilitated between literally any number of authentication sources. When leveraging SecureWithin, unlike VPN, the entire network isn't accessible, only specified endpoints like SharePoint are accessible over predetermined ports and protocols and only to authorized users. There is no need to modify the firewall settings or make any changes to the network configurations allowing organizations to stay compliant with security policies. All network traffic is outbound over port 443 SSL, which is allowed by corporate policy and proven secure.



SUMMARY

With BiTKOO organizations are able to leverage SharePoint with complete confidence and control. As users and sites multiply, manageability and security become paramount. The solution offers many deployment options and adapts to the unique requirements of your organization. It was designed to work in tandem to enforce enterprise policies across SharePoint sites and the enterprise application infrastructure.

BiTKOO licensing costs are ultra competitive. Keystone is easily deployed, highly scalable, and delivers unparalleled usability and time to value.

Test BiTKOO vs. the competition today.

BiTKOO®
 4640 Lankershim Blvd., Suite 650
 North Hollywood, CA 91602
 888.4.BiTKOO (888.424.8566)
www.bitkoo.com