

# NXT<sup>®</sup> 3 SECURITY SERVICES<sup>®</sup>

## TECHNICAL OVERVIEW

### INTRODUCTION

If information is power, then securing and protecting that information should be an essential part of any organization's asset management strategy. Controlling who has access to what information and enforcing valid authentication and authorization is absolutely necessary if information assets are to be protected--especially in a networked environment such as the Internet.

NextPage understands the critical nature of appropriately sharing information through distributed networks including intranets, extranets and the Internet. NXT 3 includes a comprehensive set of security services that enable companies to safely share varying levels of secure information with accurately identified and authorized individuals or agents.

NXT 3 Security Services<sup>™</sup> includes an access control module (ACM) that provides three levels of security functionality: authentication, authorization and metering. Authentication ensures identity of an individual; authorization matches appropriate viewing rights to that individual; and metering controls the viewing session. NXT 3 Security Services are standards based using RSA data encryption, secure sockets layer (SSL) and integrate with all standard access control mechanisms such as LDAP directories and ODBC data sources.

NXT 3 Security Services combined with NextPage's document organization and searching capabilities provide a world-class distributed information management solution. Document text, summaries, metadata and all types of search combinations are easily accessible but only to those that are authorized. Security management is made simple through hierarchical organization and nested access rights. Tight control can be maintained without extensive or complicated administration.

### NXT 3 SECURITY SERVICES FUNCTIONALITY

With the evolution of e-business, the traditional boundaries for company information repositories have dissolved. Information, often dynamic in nature, is being shared with customers, suppliers, partners, and geographically distributed offices. Where access to business critical information was once regulated by physical barriers and human control, information is now easily accessible by anyone from anywhere. The immediate problem

becomes accurately controlling who has access to what without imposing burdensome access procedures.

NXT 3 Security Services™ are enabled through the use of access control modules (ACMs). These modules work to secure business critical content and protect the relationships with e-business partners and customers by managing security policies. Security policies can be defined as the 'business rules' that determine 'who has access to what information and for how long'. Defining and enforcing these security business rules is essential for companies concerned about protecting information assets, controlling information flows and maintaining a competitive advantage.

NXT 3 Security Services encompass three areas of functionality: authentication, authorization and metering. Each of these levels of functionality work together to enable information managers to precisely control whom has access to what and how.

**Authentication** - Authentication is the process of verifying that a user is who they claim to be--verifying the credentials of a user or the user's agent. NXT 3 supports each of the several standard methods for authentication including the following:

- ACL text file - user IDs and passwords are compared against access control lists (ACLs) stored in a hashed text file
- Database - ACL information is stored as part of a secure, relational database
- LDAP Directory - ACL information is retrieved from a lightweight directory access protocol (LDAP) source or directory service
- OS Directory - ACL information comes from an operating system (NT Domains, NetWare NDS, etc.)
- Other Authentication System - access control is pre-determined using another authentication service; once verified, a positive response indicates valid authorization

The NXT 3 ACM can use any of these methods for authorization. Authentication can be performed through multiple methods such as username/password, e-mail address/password, digital certificates, etc. Included with the NXT 3 Site Administrator is a NextPage user database available for use in lieu of other existing options.

**Authorization** - Authorization is the process whereby users are granted access to specific resources. These resources (or elements of the system) include documents, applications, operations, databases, processes, etc. Authorization manages a user's access to these resources--it controls what they can see.

Mapping individual users to specific resources at any scale beyond two users becomes exponentially complex. NXT 3 incorporates a resource and user hierarchy that greatly simplifies the task of managing authorization. Resources or system elements can be placed in a hierarchy (or table of contents) so that access can be granted for one or many elements. Access might be granted to a 'directory' element and in turn all 'files' within that directory would also be accessible.

Users can be granted access through the use of groups or roles. Pre-defined access might be granted to a specific 'role' such as 'department head' that allows them to see all department budget information. Assigning an individual user to the 'department head' role would, in a single effort, grant them access to all information appropriate for department heads. 'Group' membership in a 'sales' group would allow any sales group

member to see all relevant sales information such as pricing, spec sheets and inventory levels.

The combination of hierarchical user and resource management provides a powerful authorization solution. Access to resources can be specifically assigned and matched to individual users--or--classes and subclasses of resources can be authorized for roles or groups of users.

The process used with NXT 3 to enable group access is to set up 'views' to information. Views might include a database query set, a directory, a Web site or a group of files. Once views are established, group access can be granted. A user may switch between multiple views without needing to re-authenticate.

Authorization also includes the application of an approved set of permissions or roles for a user. The standard set of permissions is 'view content', 'view metadata', 'navigate', 'query', and 'edit'. These permissions define the level of activity that an authorized user may participate in. Customers may be able to 'view' a price list document but only the 'sales manager role' would have permission to 'edit' it. Again, role or group information can be obtained from an LDAP directory or other authentication databases.

**Metering** - Metering is the process whereby once authentication and authorization have taken place, access to the resource is further controlled based on a defined set of metrics. This management or control can be based on any one of several criteria including time limits on access, limits on the number of page views, limits on concurrent users, etc.

For example, an analyst service might offer a 'try and buy' option that allows a potential client company to view a marketing report five times for free but after that requires remuneration. Users might buy services that allow them to have access to a data repository for a limited number of hours per month for a minimal fee.

Metering can also be used to gather usage statistics that are valuable in providing reporting and accounting services. Statistics can be gathered that track facts such as: number of documents requested by a particular user, number of times a document is accessed, the number and makeup of search requests, the amount of system resources used, system usage over time, etc. Metering services can be used to calculate usage and cost based resources.

In addition to these three areas of security functionality, NXT 3's access control modules incorporate industry standard methods for security. In environments where a secure transmission over the Internet is desired (either for access or management), NextPage uses RSA data encryption and SSL. RSA is the industry standard for public key/private key encryption that enables the management of encrypted data transmissions without excess management requirements. Digital signatures are created for users which include a public key and a private key. The public key is used to encrypt data and the private key is used to decrypt it with mechanisms to ensure that the data has not been opened or tampered with.

SSL is the leading security protocol for the Internet. Internet servers work with Web browsers to generate a unique session key that is used to encrypt all data transmitted during the active session. This ensures that information passed back and forth is secure. Robust security services provide the foundation necessary to manage and protect digital content.

NXT 3 is managed through a Site Administrator console. Authentication and authorization parameters and users can be configured using a graphical user interface where users, groups and access to resources can all be defined. Metering functionality is available via a C++ API interface that can be flexibly customized to meet any type of statistical management need.

## CONCLUSION

Digital assets require protection--especially in a distributed environment. The ability to provide adequate security without undo hardship to users is key to establishing a viable information sharing solution. NextPage accomplishes this balance successfully with the authentication, authorization and metering capabilities built into NXT 3.

The advantages of a robust but secure information publishing system are significant to any organization establishing an e-business presence. NXT 3 benefits include the following:

- ***Precision Information*** - Users only see information that is authorized and relevant to them.
- ***Simplified Management*** - Availability and access to information is simplified through the use of resource and user authorization.
- ***Ease of Integration*** - NXT 3 solutions integrate with established security methods and mechanisms such as LDAP, RSA, SSL and standard relational databases.
- ***Complete Security*** - Security is applied to all digital assets including documents, applications, directories, processes, operations and services.
- ***Distributed Environment*** - NXT 3 enables the aggregation and sharing of information through any distributed environment including intranets, extranets and the Internet.

In conclusion, NextPage helps organizations secure business critical content and helps protect relationships with e-business partners. NXT 3 enables the secure delivery of the right content to the right user, every time.