INFOSHEET

NEXJ CRM SECURITY OVERVIEW

NexJ offers a dynamic, flexible, extensible, and centralized security model that allows information to be shared across the enterprise according to specified visibility rules. Security rules are enforced by the NexJ Server and are centrally defined in the Business Domain Model, so they will be consistently applied regardless of the UI or access methods being used to retrieve or manipulate data elements. This means that different groups throughout your organization can use one instance of NexJ CRM across lines of business while maintaining the business processes that are unique to each.

This document explains NexJ's robust security model, and its four components.

NexJ's security model is fully customizable without compromising the ability to upgrade the software. It's built on industry standards that allow NexJ to map directly to existing security models and consume an existing entitlements model that encapsulates client preferences and regulations.

NexJ's security model has the following four components:

Integrated User Authentication

User authentication determines who someone is and if they're allowed to access the system.

NexJ enforces authentication using an adapter-based approach. Because NexJ's security model is based on industry-wide standards, NexJ is able to map directly to existing security models and consume existing entitlements models. The NexJ Enterprise Application Platform supports pluggable security adapters, and extensible synchronization technology. This enables NexJ to create custom or standardized adaptors for user authentication, or to integrate with custom authorization information.

NexJ supports the ability to authenticate against a user registry that is defined internally or an enterprise user registry maintained externally. NexJ leverages the Java Authentication and Authorization Service (JAAS) in the Java EE infrastructure. This allows the NexJ application to remain independent from underlying authentication technologies and plug into existing authentication patterns clients may already employ. New or updated technologies can be plugged in without requiring modifications to the application itself.

NexJ has deployed across a range of technologies in customer environments, including LDAP, Active Directory, CA SiteMinder, Tivoli, SPNEGO, Kerberos, WebSEAL, and OpenAuthentication. These systems provision user roles and allow dynamic auto-assignment of privileges to NexJ users.

Data Visibility

Data visibility determines what a user can see in the system.

NexJ's Data security capabilities are extremely powerful as they are dynamic and can include logical rules that are based on the data being viewed, attributes of the user, or even external input. Data level security is used to control access to object instances or records. NexJ supports three different levels of privacy for viewing and editing any item:

- Public – items can be viewed by all users
- Group – items can be viewed by a subset of users, or a group of users
- Private – items can only be viewed by one specific user

Additionally, the group and private levels of security can be blended with other business requirements to address client-specific needs. For example, this could allow all branch managers to view private items that are linked to their branch.

Because security is defined centrally, all data access methods automatically subscribe to the same centrally defined rules. This architecture allows the NexJ Enterprise Application Platform to easily integrate with customized or proprietary security models and user profiles.

All data can be controlled in terms of access. For example, any data deemed as Highly Confidential can be restricted to access based on entitlements. These restrictions can include making data read-only, masking the data, or hiding the user interface elements entirely.

Functional Entitlements

Functional entitlements determine what a user can do in the system.

In NexJ, functional entitlements define security concepts such as user roles, groups, and privileges. Users are associated with privileges that allow or deny access to functionality, broad data actions, or specific attributes, screens, tabs, controls, or fields within NexJ CRM. Users can also be assigned roles and groups that segment them into categories with specific privileges. This allows role or group assignments to control object access capabilities for different users.

This amount of specification provides a high degree of functional decomposition and granularity by user role, such as institutional sales, trading, or research. Additionally, user role assignments can be used to determine things like screen layouts and default values. NexJ also offers the ability to assign multiple security roles to users. This allows customers to offer multiple security role assignments simultaneously, or to force users to choose the role they want to operate under at any given time.

Encryption

Encryption means that data is secured both at rest, and in transit.

NexJ uses industry standard JDBC libraries to connect to database servers. This allows us to utilize the existing information security processes provided by these systems to comply with FISMA and similar standards where applicable. For data located on the application server tier, including batch files, non-database queues, and log files, these items are secured and/or encrypted with industry standard processes provided by the operating system and similar facilities.

For data in transit, NexJ uses Transport Layer Security (TLS) or Secure Socket Layer (SSL) to secure customer communications over the network. NexJ ensures that all data is encrypted internally before it is available for remote access. Server to server communications can be configured to use mutually authenticated certificates, which can include encryption. The NexJ Server locally stores database access credentials in an optionally encrypted format, thus those credentials are never communicated via web services. For integration channels, NexJ optionally supports mutual certificate authentication.

NexJ's comprehensive security model provides our customers with the flexibility to meet any security requirement and to mirror how your business works across roles and job functions, asset classes, and lines of business.

To learn more about how NexJ Systems can help you meet your security requirements, visit **www.nexj.com** or email **info@nexj.com**

NexJ Systems Inc.
10 York Mills Road, Suite 700,
Toronto, Ontario M2P 2G4
P: 416 222 5611 F: 416 222 8623
info@nexj.com www.nexj.com

About NexJ Systems

NexJ Systems is a provider of Intelligent Customer Management software for the financial services industry. The Intelligent Customer Management suite is comprised of NexJ's award winning-products that use artificial intelligence to optimize customer management and increase advisor productivity, and cognitive applications that use machine learning to recommend the right actions to work smarter and faster.