Integrated Authentication

Information Security Introduction

Information security has become an increasingly visible and important topic to companies. Driven by a number of highly publicized security breaches and episodes of financial malfeasance, organizations are under pressure to implement the business processes and technical infrastructure necessary to protect their information assets. In most cases, information assets are stored in relational database systems and accessed by customers, partners, and employees using business applications such as financial reporting systems, e-commerce websites, and employee and partner intranets. Many of these business applications are deployed using Java, which leverages JDBC driver technology for connectivity to the database. In order to protect information assets, each component of the application infrastructure must be secure; otherwise, the information asset may be compromised. This document explains the role that a JDBC driver plays in a secure solution and explains how DataDirect Technologies is taking a leadership role in ensuring secure database access through JDBC.

Industry Drivers

A number of industry factors have increased the level of scrutiny relative to information security. These factors include:

- Internet-based World-Wide Collaboration – ubiquitous access to information spanning the traditional enterprise border has led to increased privacy concerns.
- Financial malfeasance – highly visible corporate failures have resulted in increased government oversight.
- Regulatory Compliance – a series of new regulatory requirements have been introduced that have forced organizations to implement additional security policies.
- IT Management Cost Containment – many IT organizations are tasked with reducing the costs necessary to manage a secure infrastructure.
- Application Usability – company expectations of their developers to deploy highly secure applications without jeopardizing the usability of the application.

These industry factors require IT organizations to implement security processes and systems that:

- Bolster the application data and authentication security
- Improve the manageability of the user account information
- Lower the cost of account and password maintenance
- Ensure a high level of security without adversely impacting user experience

Regulatory Compliance

In particular, regulator compliance is becoming an increasing concern. Driven by financial malfeasance (e.g., Enron, WorldCom) and numerous data breaches (e.g., LexisNexis, Ameritrade), government regulators have stepped up their level of due diligence with regard to financial reporting and information security. Additional federal and state level regulations have been enacted that increase the level of corporate and personal liability for publicly traded companies. In addition, the government is more aggressively holding organizations accountable based on existing legislature. While some of these regulations are focused on financial transparency (e.g., Sarbanes-Oxley, Gramm-Leach-Bliley, Basel II), others are focused on data privacy (The Data Protection Act 1998, California Privacy Act). For the most part, the financial reporting regulations require that organizations establish and maintain internal controls over financial data. The data privacy regulations are focused on protecting personal identification information, ensuring that organizations notify customers if a security breach occurs, and restricting e-mail, fax and text message advertising.

Let's take a closer look at Sarbanes-Oxley or SOX. In financial reports to the SEC, SOX requires that a company's CEO and CFO certify that they have established and are in the process of maintaining internal controls that ensure that upper-level management reports accurate and truthful information about the company's finances and operations. SOX provides a set of business-level guidelines that define the business processes and executive accountability required to ensure shareholder value. These guidelines are general in nature and do not specify the process implementation method, nor do they provide specific guidance in terms of IT security. Organizations must interpret the regulations and implement the policies and procedures that they deem necessary to satisfy SOX.

Although the requirements necessary to support compliance are subject to interpretation and vary based on the size and complexity of the organization, it is clear that a number of technical features must be implemented to support regulatory compliance efforts. Regardless of the regulatory requirements,

these features would bolster IT security while providing a best-practice approach for IT governance. These features include:

- Integrated Authentication (Single Sign-on)
- Consolidated Account Management
- Comprehensive Information Audit
- Secure User Credential Transmission

See the addendum at the back of this paper for a discussion of each of these security features plus a discussion of multiple sign-on vs. integrated authentication.

Kerberos / NTLM Protocol Overview

Most relational database systems support multiple security authentication mechanisms. The options typically include native database authentication as well as OS authentication. OS authentication provides the mechanisms (security and account) necessary to securely authenticate the user. By allowing the database to share the network user name and password, users with a valid network account can log onto the database without supplying a user ID and password. In addition to Single Sign-On within a network domain, OS authentication provides a more secure mechanism for logging on the database server. Standard network security mechanisms also provide the added advantages of auditing, password aging, minimum password length, and account lockout after multiple invalid login requests.

Kerberos

DataDirect Technologies has implemented its support for OS authentication using Kerberos, an authentication protocol that is an integral component of Windows Active Directory. Since Windows 2000, the Kerberos protocol is the default authentication package in a Windows environment. In addition, DataDirect supports Microsoft's NTLM (NT LAN Manager) protocol, a challenge response mechanism that is the default for network authentication in Windows NT 4.0. Microsoft has retained support in Windows 2000 for compatibility with earlier client and server versions of Windows.

Kerberos is designed to provide authentication using secret key cryptography. Kerberos is based on the RFC 1510 standard, which ensures interoperability between implementations. This is especially important in environments that leverage a combination of client platforms (e.g., Windows, UNIX, Linux). Kerberos is more flexible, efficient, and secure than other authentication methods. The Kerberos protocol is ideal for applications that share data over the Internet because Kerberos eliminates the need to pass user ID and password information over the wire, ensuring greater security. Kerberos also detects whether the user credentials were modified while in transit over the network. The DataDirect Connect *for* JDBC SQL Server driver is the only JDBC

driver on the market that supports Windows authentication while remaining a pure Type 4 JDBC driver. DataDirect Technologies even has a patent pending on this innovative technology. DataDirect's solution implements Windows authentication without loading external shared libraries (DLLs on Windows). Drivers that load external shared libraries are considered Type 2 drivers, because they are not pure Java®. A pure Java solution is important to many Java developers because using Type 4 drivers, such as DataDirect Connect *for* JDBC, eliminates the need to install database-specific client libraries or additional shared libraries, which results in less setup and maintenance for deployed drivers. An added benefit of using Type 4 drivers is that they use the database wire protocol directly, which can help boost performance.

NTLM Protocol

Although the Kerberos protocol is the preferred authentication mechanism, DataDirect also provides a Type 2 implementation based on NTLM in order to meet the diverse needs of the enterprise IT market. In some cases, NTLM is the method of choice based on application infrastructure design, configuration complexity, and Windows operating system version levels. The NTLM protocol is a Microsoft supported challenge-response mechanism that provides a subset of the functionality enabled by Kerberos. Although it only provides a subset of the functionality enabled by Kerberos, it represents a significant improvement in security as compared to the native database authentication mechanism. NTLM remains a viable option for environments that do not require the rigor, interoperability, or advanced functionality provided by Kerberos.

DataDirect OS Authentication Feature Overview

If an organization is attempting to deploy a SSO infrastructure or taking steps to consolidate their authorization design, each component of the application stack must play a supporting role. Each component, including the database, operating system environment, application code, application/web servers, as well as the database driver, must support SSO capability to deploy a completely integrated authentication solution. DataDirect provides the following capabilities as part of DataDirect Connect *for* JDBC in order to provide support for multiple authentication designs.

IMPORTANT: Please note that the availability of these capabilities is dependent on the operating system / database environment. Contact DataDirect to discuss your specific requirements.

Authentication "Pass Through"

Although the database driver does not dictate the authentication methodology to be used by the application, it is imperative that the driver supports the various designs that are leveraged in today's Java-based application environments. To meet the technical needs and application design of various enterprise environments, DataDirect designed the DataDirect Connect *for* JDBC driver family to support an industry first, "Pass Through" authentication capability. This approach ensures that the DataDirect Connect *for* JDBC driver can support the design of virtually any application environment; including Kerberos and NTLM protocols, Active Directory and MIT KDC's, user delegation capability, diverse technical topologies (databases, application client platforms), etc. The driver can be configured to automatically determine the authentication method based on environment characteristics (more on this later) vs. imposing a rigid, inflexible design approach.

Credential Delegation

DataDirect Connect *for* JDBC supports the ability to delegate a credential through the application stack. In Single Sign-on environments, the application authenticates the user using the Windows user credential in combination with an authentication protocol (e.g., Kerberos, NTLM). The application then delegates the user credential to the next component in the stack (the JDBC driver) in order to access the database. The DataDirect delegation capabilities allow the database to authenticate the user via the delegated credential as opposed to a separate, non-integrated user ID.

NTLM / Kerberos Support

DataDirect supports both the Kerberos and NTLM protocols. This flexibility allows an organization to design their authentication approach based on their

business and technical needs, instead of based on the constraints of the JDBC driver. As explained in this paper, these protocols provide the framework for the following benefits:

- Consolidation of user IDs
- Secure transmission of user credentials
- Elimination of duplicate account data

Extensive Database and Platform Support

DataDirect supports an extensive set of databases (e.g., Microsoft SQL Server, Oracle, etc.), multiple application client environments (e.g., Windows, Linux, UNIX), multiple protocols (NTML, Kerberos) as well as multiple Kerberos environments (Active Directory, MIT Kerberos). This extensive level of support ensures that a single JDBC driver solution can meet the needs of a heterogeneous enterprise-wide environment.

DataDirect Authentication Deployment Overview

Since the DataDirect Connect *for* JDBC drivers provide multiple options for authentication, an organization must select the authentication mechanism for the application. The security and usability needs of the organization along with the technical infrastructure dictates the preferred authentication approach. DataDirect provides extensive documentation that explains the setup and configuration process for authentication (refer to "DataDirect Authentication References" later in this paper). This document provides a general introduction into the authentication deployment methodology. In addition, the level of support provided for OS authentication varies by database and operating system. Your account manager can provide information about how the DataDirect capabilities map to your specific environment.

The following factors impact your choice of authentication method:

Authentication Factor	General Recommendation
Risk Assessment	Applications with stringent security requirements should opt for the Kerberos-based authentication option. This option provides the highest level of security compared to NTLM or database authentication.
Application Usability	Applications that require an optimal end user experience should rely on a SSO deployment based on Kerberos / NTLM. This eliminates multiple user logins along with the burden of managing multiple user ID / password combinations.
Deployment Management	Organizations that are averse to managing client components on the machine hosting the application should opt for a Type 4 solution. This eliminates the need to deploy Windows-specific client components that are required for a Type 2 solution.
Network Topology	The Type 4 Kerberos-based solution requires Windows Active Directory. In addition, the network topology must be designed so that the same domain controller administers the database server and application client.

Authentication Factor	General Recommendation
Database / Client / J2SE Version Requirements	The authentication method selected must account for the database, client, and J2SE release levels. The Kerberos and NTLM protocols necessitate a certain level of database, client and J2SE release versions to work properly.
Configuration Complexity	The Type 4 Kerberos-based method requires more configuration than the Type 2 solution because it is necessary to configure Active Directory for Kerberos support.

Once the authentication method has been determined, the AuthenticationMethod connection property of the DataDirect Connect *for* JDBC drivers is used to configure the type of authentication that the driver uses. This connection property provides an "auto" capability that allows the driver to determine the authentication mechanism based on criteria available to the driver. This criteria includes information about the user ID (whether it is provided or not), the client platform (e.g., Windows or non-Windows), and accessibility to the Type 2 DLL. The driver can also be configured to use a specific authentication method by explicitly stating "type2", "type4" or "none" (database authentication).

To complete the Kerberos / NTLM implementation, the database, domain controller, and application client also need to be configured. For a complete overview of this configuration, refer to the configuration steps documented in the *DataDirect Connect for JDBC* documentation.

Summary

Organizations are feeling the pressure to improve their IT security infrastructure. This pressure is the result of several industry drivers including the proliferation of the internet, highly publicized corporate financial malfeasance / security breaches, and increased government and legislative regulation. At the same time, organizations must strike a proper balance between application usability, user convenience, and management cost vs. the security requirements. To achieve a high quality application solution with robust security, many organizations are moving to support integrated authentication solutions based on SSO. This approach includes support for consolidated account management, comprehensive information auditing, along with secure user credential transmission. To realize this security capability, every component within the application stack needs to be designed to support the concept of Windows authentication. The DataDirect Connect *for* JDBC family of drivers provides the capabilities and flexibility necessary to implement an integrated authentication solution. The DataDirect authentication "Pass Through" capability, combined with our ability to support credential delegation, can be used to implement an enterprise-wide integrated authentication solution based on our extensive support for various technical infrastructures (support for Kerberos/NTLM protocols, Type 2 / Type 4 drivers, heterogeneous database and client applications).

Please contact DataDirect Technologies to learn more about this critical security feature and other industry leading features provided by DataDirect Connect *for* JDBC family of drivers.

DataDirect Authentication References

DataDirect Connect for JDBC Installation Guide

DataDirect Connect for JDBC User's Guide and Reference

(http://www.datadirect.com/techres/jdbcproddoc/index.ssp)

Windows Authentication on Microsoft SQL Server

(http://www.datadirect.com/developer/jdbc/topics/winauth/index.ssp)

Addendum

Integrated Authentication (Single Sign-on)

End users and IT professionals alike are all too familiar with the process of logging on the corporate network, then initiating and logging on each application separately. Given the number of applications that are used in corporate settings, today's user is responsible for managing an increasingly large set of user ID / password combinations. To complicate matters, each application has its own set of rules for password format, maximum password age, password history rules, etc. Multiple user ID/password combinations result in users writing them on paper that is left in close proximity to their work stations, which greatly increases the security vulnerability of the applications. The other side affect is that lost passwords or login problems result in a flood of calls to the IT Help Desk. Some studies show that as many as 45% of the help desk calls are related to password resets. This translates into a significant amount of IT support dollars and lost productivity time for the end user.

Contrast this situation with a Single Sign-on (SSO) environment. The user logs on the network, the network operating system authenticates the user, and the user initiates the necessary business applications. If the applications are integrated into the SSO environment, users are not prompted for a user ID / password, they simply start the application. The application works in concert with the network operating system to authenticate the user based on the user's credential associated with the network login. This approach results in improved end user productivity, lower IT management costs relating to password and login issues, and an improvement in the overall security posture of the application environment.

Consolidated Account Management

Today's application environments are very dynamic. New applications are constantly being deployed, while existing applications are frequently modified. In addition, the responsibilities of end users are ever changing. Companies are acquired; companies merge; departments are realigned; and employees start jobs, change roles, and terminate their positions. These changes need to be reflected in the application environment to ensure that only authorized people have access to application data. Without SSO, organizations replicate user account data in multiple databases. The user account data necessary to control network access is stored in a network directory such as LDAP or Active Directory, while account data for each application is stored in a proprietary format in the application database. For every business change (e.g., new employee, job transfer, job termination, department realignment, etc.), IT is forced to modify the user information in each account database using a variety of different tools and user interfaces. In addition to the management costs associated with this approach, a much higher level of security risk is assumed if the account data is not maintained on a timely basis.

SSO ensures that organizations use a single repository to manage user account information. In a Windows environment, user account information is stored using Active Directory, which supports the Kerberos protocol that can be used to implement SSO (same thing for UNIX/LDAP). This eliminates the need to store duplicate user account information and for separate, proprietary authentication vehicles for each application. Consolidating the account data greatly reduces the cost associated with user management and improves the overall security posture of the application infrastructure.

Comprehensive Information Audit

SSO allows the authentication design to support the concept of delegated credentials. This simply means that the user identity is passed through to each component supporting the application. In environments that do not leverage SSO, it is not uncommon for the application server to leverage a generic user ID in order to log into the database. The actual user ID and password are then validated using a proprietary method, but they are not used to log into the database. The generic user ID poses a significant security exposure because it has to be stored and retrieved by the application code in order to establish a connection to the database. In many cases, the generic user ID is stored in a configuration file that is virtually unprotected. The other problem with this approach has to do with the auditing or logging capability of the database. In most cases, databases log the user ID with the database activity (e.g., inserts, updates, etc.). If a generic user ID is associated with the database activity, the actual user information is obfuscated, which greatly reduces the value of the audit. Some applications provide additional code so that the database activity can be associated with the actual user, but this requires additional design work, development time, testing, and monitoring capabilities.

In a SSO environment that leverages delegated credentials, the user identity is securely passed through the web, application, and database server components involved in supporting the application. This allows each component of the application to associate application activity with the actual user vs. a generic ID. In addition, elimination of the generic ID increases the overall security level of the application since the generic ID cannot be compromised.

Secure User Credential Transmission

In addition to usability and IT management issues, relying on each application to authenticate the user results in a lower level of security. This is due to the fact that most applications (packaged and custom) typically implement a rudimentary approach to authentication. In most cases, user ID / password information is transmitted across the network. Information is transmitted in clear text or using simple encryption mechanisms including text obfuscation (e.g., Base64 encoding).

For SSO environments that leverage the Kerberos protocol to perform authentication, the user ID / password are not transmitted across the network. Instead, industry standard encryption is used to pass credentials that uniquely identify the user between the application and operating system components to authenticate the user. Unlike user ID / password, if these credentials are intercepted, there is virtually no likelihood that they can be used to compromise the application. This is due to the fact that the Kerberos protocol leverages a bi-directional handshake mechanism between the client, KDC, and server components. This eliminates the ability for a perpetrator to record and replay the authentication credential stream, which is a real threat in authentication paradigms that transmit user ID / password.

Multiple Sign-on vs. Integrated Authentication

Let's take a look at a before and after view of security with respect to the previously discussed security features in a Windows environment. In a non-integrated environment, a user starts Windows and is prompted for a user ID/password. The Windows operating system (usually in conjunction with a domain controller and Active Directory) authenticates the user and provides access control to network resources. After the user is logged in, the user starts a business application and is prompted for another user ID/password. The user enters his user ID/password and the application authenticates the user using a proprietary, application-specific authentication procedure. This authentication procedure typically involves using:

- A generic login ID to connect with the application database
- Rudimentary encryption of the user ID/password
- User validation against a list of application-specific user IDs

In addition, the database access necessary to support the application is not associated with the user (unless the application includes additional logic that

compensates for this shortcoming) since a generic database user ID is used. This process of application authentication is then repeated for each application that the user starts.

In contrast, an application environment that leverages an integrated authentication approach works as follows. The user starts Windows and is prompted for a user ID/password, which the Windows operating system uses for authentication. Once authenticated, the user starts a business application. The user is not prompted for another user ID/password since the application (via the Kerberos protocol) uses Windows-based network facilities to determine the validated network user name. The application, database server, and the Key Distribution Center (KDC) running on LDAP interact using the Kerberos protocol to authenticate the user. Integrated authentication eliminates the need for multiple user IDs, logins, and account databases and replaces the transmission of user ID/password with hardened, Kerberized credentials. In addition, since the user credential is used for the database authentication, database activity can be associated in the logs with the end user vs. a generic user ID.

Although the Windows operating system is used to illustrate this example, the same basic scenario applies in a UNIX environment that leverages LDAP as the directory server.

The following table highlights the benefits of an application environment that leverages integrated authentication:

Multiple Sign-On	**Integrated Authentication**	**Benefit**
User IDs & passwords are sent across the network	Authentication enabled via shared secrets / encryption	Eliminates security vulnerability
Multiple User IDs and System IDs required	Single User ID and elimination of System IDs	Eliminates usability issues while strengthening security
Duplicate user information in multiple account databases	Single store of user account credentials	Reduced management costs and better security
Database activity logged with generic System ID	Database activity identified by User ID	Better audit accuracy assists compliance efforts

We welcome your feedback! Please send any comments concerning documentation, including suggestions for other topics that you would like to see, to:

docgroup@datadirect.com

FOR MORE INFORMATION

800-876-3101

Worldwide Sales

Belgium (French) 0800 12 045
Belgium (Dutch) 0800 12 046
France 0800 911 454
Germany 0800 181 78 76
Japan 0120.20.9613
Netherlands 0800 022 0524
United Kingdom 0800 169 19 07
United States 800 876 3101

DataDirect TECHNOLOGIES

DataDirect Technologies is focused on data access, enabling software developers at both packaged software vendors and in corporate IT departments to create better applications faster. DataDirect Technologies offers the most comprehensive, proven line of data connectivity components available anywhere. Developers worldwide depend on DataDirect Technologies to connect their applications to an unparalleled range of data sources using standards-based interfaces such as ODBC, JDBC and ADO.NET, as well as cutting-edge XML query technologies. More than 250 leading independent software vendors and thousands of enterprises rely on DataDirect Technologies to simplify and streamline data connectivity. DataDirect Technologies is an operating company of Progress Software Corporation (Nasdaq: PRGS).

www.datadirect.com