

# SafeJDBC

## Strong Encryption of SQL Data Technical Brief

Nicolas de Pomereu – Associate Director

SafeLogic – 27–29, rue Raffet - 75016 Paris - Tél : (33) (0)1 45 72 25 15  
<http://www.safelogic.com>

# SafeJDBC – A JDBC Driver Providing Strong Encryption

## Outline:

- ▶ **SQL Data: Overview & Risks**
- ▶ **SQL: Standard Solutions for Protecting Data**
- ▶ **SafeJDBC - Objectives**
- ▶ **Flow Diagrams**
- ▶ **Technology**
- ▶ **SafeJDBC for Windows (SafeODBC)**
- ▶ **SafeJDBC for Oracle/OCCI**
- ▶ **Advantages of SafeJDBC**

# SQL Data: Overview and Risks

## Strategic SQL data and security threats:

- ▶ **Customer database**
  - ▶ Content: customer contact information.
  - ▶ Threat: competitors.
  
- ▶ **Employee database**
  - ▶ Content: histories, salaries, private data ...
  - ▶ Threat: hostile employees.
  
- ▶ **e-commerce**
  - ▶ Content: credit card numbers, transactions.
  - ▶ Threat: Internet hackers.

# SQL: Standard Solutions for Protecting Data

## 1. Protective measures offered by SQL vendors:

- ▶ userid/password required to log in.
- ▶ Privileges managed with GRANT/REVOKE.
- ▶ SSL connection between application and database.

**These measures protect access to the database, but not to the unencrypted files that contain the data:**

- ▶ Content attacked through the Internet or network.
- ▶ Hard drives can be stolen or copied...

# SQL: Standard Solutions for Protecting Data

## 2. Encrypting the system partition:

- ▶ A data partition on the hard drive is encrypted. It is protected by a secret key.
- ▶ The partition is encrypted at shutdown → Impossible to steal data when the machine is off.

### **BUT...**

- ▶ The SQL data are still accessible and unencoded when the system is running:
  - ▶ The risk of data theft via the network is still present.
  - ▶ An attacker who has physical access to the server can copy the unencoded contents of the hard drive when the machine is on.

## SQL: Standard Solutions for Protecting Data

### 3. Encryption interface between the SQL data and the application:

- ▶ Reliable solution.
- ▶ Sensitive data are always in encrypted form in the SQL database, whether the machine is on or off.
- ▶ The application uses a key to encrypt and decrypt data on the fly.
- ▶ If network intrusion or theft of the hard drive occurs, the content is unusable.

## Application Encryption of SQL Data

**An encryption interface between the SQL data and the application can be developed.**

**BUT...**

- ▶ The development efforts require encryption specialists.
- ▶ Such development is complex.
- ▶ It must work within production and performance constraints.

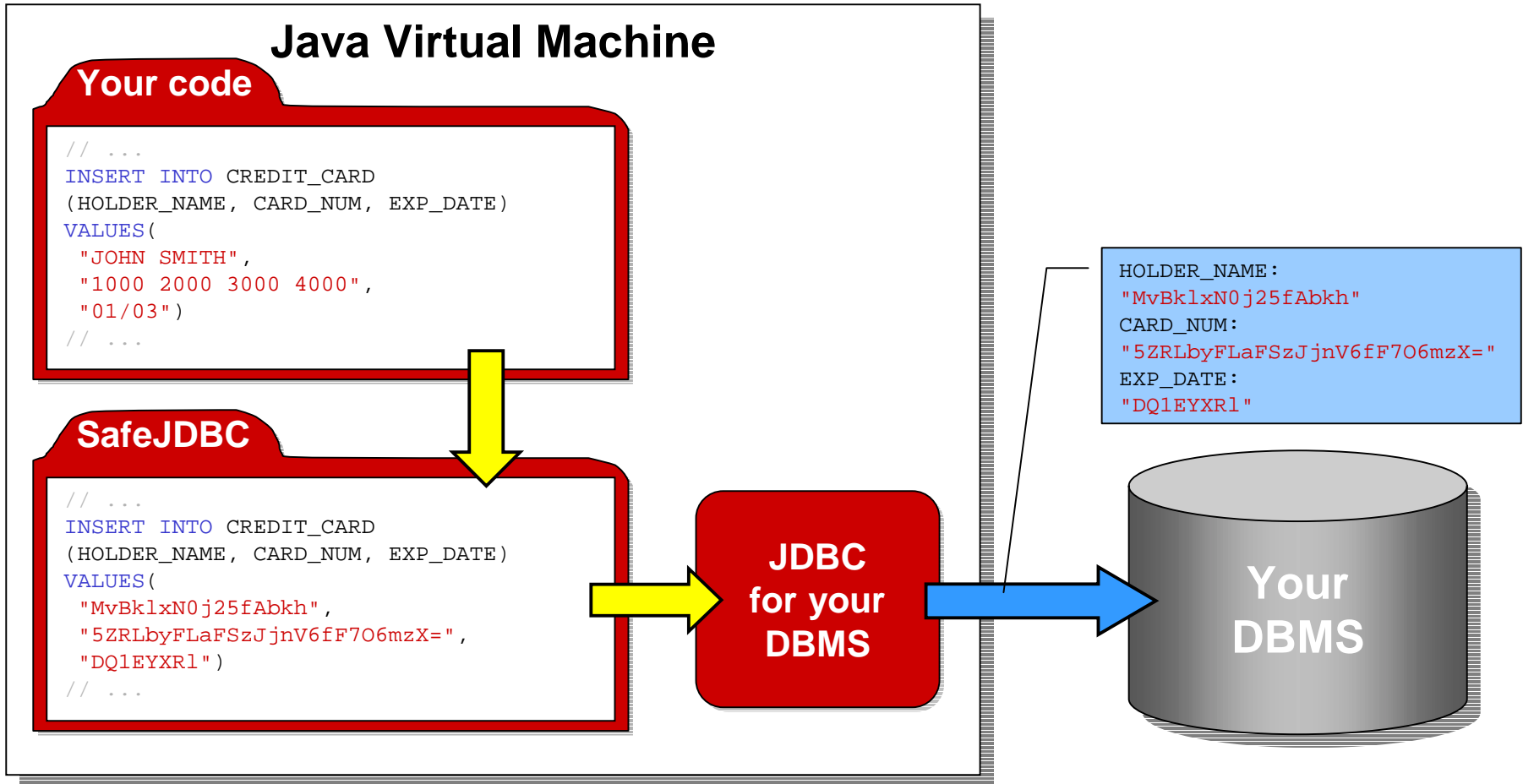
**What solution overcomes these disadvantages?**

# SafeJDBC - Objectives

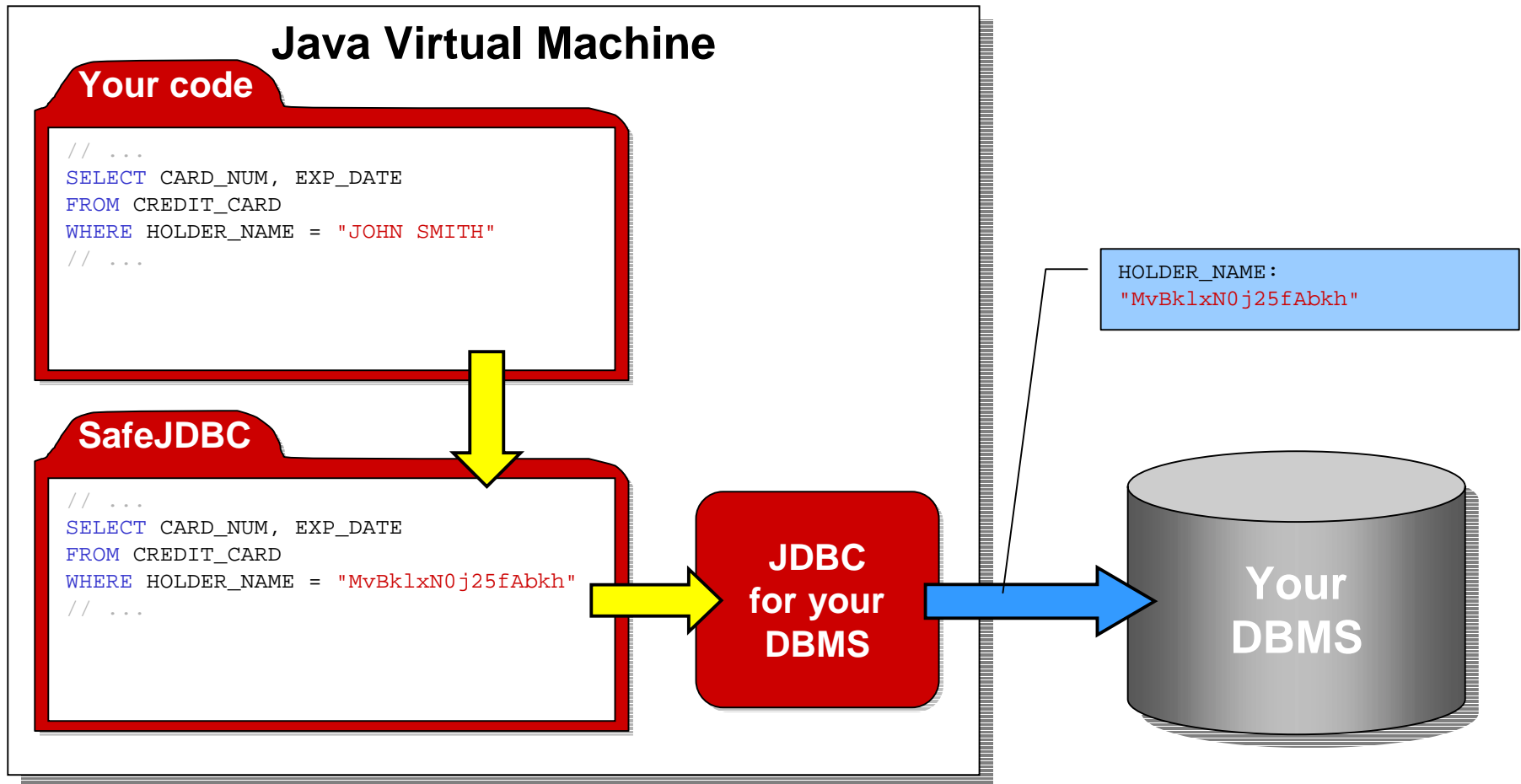
**Three main objectives:**

- 1. Use strong encryption to protect and secure sensitive SQL content.**
- 2. Integrate with Java applications immediately: no additional code required.**
- 3. Integrate into the production chain without adding overhead to the SQL DBMS.**

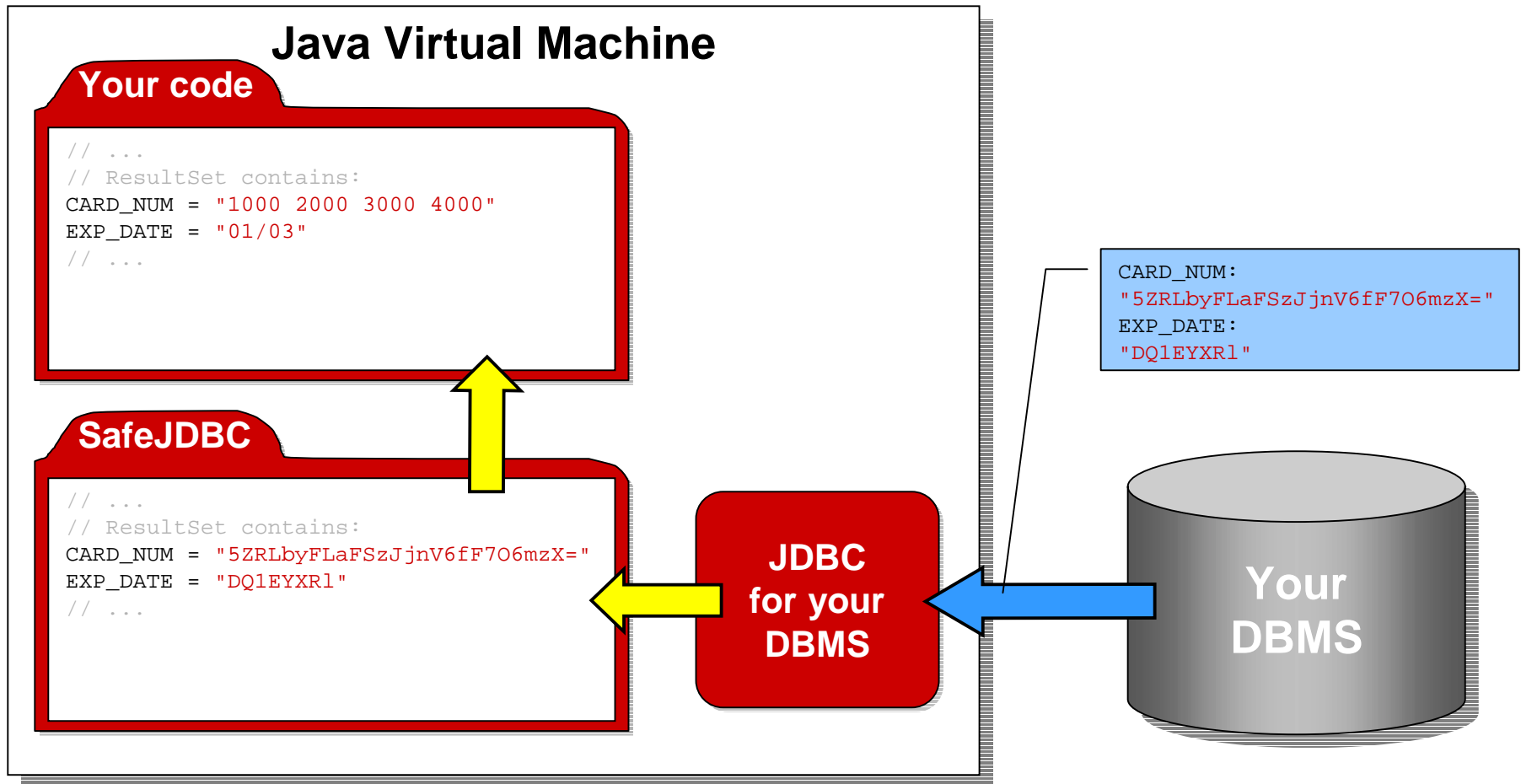
# Inserting Data



# Retrieving Data: step 1/2



# Retrieving Data: step 2/2



# Technology

## Main characteristics:

- 1. Plug-and-play integration with existing Java code: no additional development required.**
- 2. Runs with any SQL DBMS that has a JDBC 2.x or 3.0 driver.**
- 3. Runs with major J2EE Application Servers.**
- 4. Accommodates SQL data handling constraints (reliability and performance).**

# Technology

## 1. Plug-and-play integration with existing Java code: no additional development required

- ▶ No change to the existing code:
  - ▶ ONE command to load the JDBC driver.
- ▶ Deployment guarantee:
  - ▶ Simple, flexible, fast
  - ▶ No side effects or bugs.

# Technology

## 2. Runs with any SQL DBMS that has a JDBC 2.x or 3.0 driver

- ▶ Compatibility with your JDBC driver:
  - ▶ SafeJDBC encapsulates existing JDBC drivers - as a gateway with no performance overhead.
  - ▶ Runs with DB2, Informix, MySQL, Oracle, PostgreSQL, SQL Server, Sybase, ...
- ▶ Long term investment:
  - ▶ SafeJDBC will integrate with future drivers.

# Technology

## 1. Runs with major J2EE Application Servers

- ▶ **JNDI and DataSource support (JDBC 3.0).**
- ▶ **Supported Application Servers:**
  - ▶ BEA WebLogic,
  - ▶ IBM WebSphere,
  - ▶ JBoss,
  - ▶ Sun iPlanet,
  - ▶ Jakarta Tomcat.

# Technology

## 3. Accommodates SQL data handling constraints

- ▶ **No** accessing the SQL catalog.
- ▶ The **encryption** operations all occur in the **space of the JVM** (Java Virtual Machine).
- ▶ Storage of encrypted SQL data causes **no additional traffic** between the JVM and the SQL engine.
- ▶ Little or no performance overhead for the SQL engine.

# Technology

## ▶ Factsheet/Features:

- ▶ Java 1.4 in Windows NT/2000, Linux, and Unix.
- ▶ Compatible with any JDBC 2.x and 3.0 driver.
- ▶ Uses the SafeAPI encryption engine (certified by DCSSI and audited by Cryptolog).
- ▶ Encryption with long keys (128 bit).
- ▶ Choice of algorithms:
  - ▶ Standard: Blowfish.
  - ▶ Optional: CAST, IDEA.

# Technology

## ▶ Factsheet/Features:

- ▶ Transparent management of secret keys:
  - ▶ Passphrase protection (long password).
  - ▶ Possibility of secret keys that are not stored.
  
- ▶ Formats
  - ▶ INTEGER,
  - ▶ CHAR, VARCHAR, LONGVARCHAR,
  - ▶ BINARY, VARBINARY, LONGVARBINARY,
  - ▶ Large Objects : BLOB, CLOB.

# Technology

- ▶ **Factsheet/Features:**
  - ▶ SQL 2 compatibility:
    - ▶ Standardized commands DELETE, INSERT, SELECT, UPDATE.
    - ▶ Allows joins between encrypted SQL columns.
  - ▶ API and interface for switching existing applications over.
  - ▶ Unencrypted rollback management.
  - ▶ If needed: SafeLogic consulting and services.

# SafeJDBC for Windows (SafeODBC)

- ▶ **SafeJDBC for Windows:**
  - ▶ ODBC Driver .
  - ▶ Pure ODBC wrapper (DataSource).
  - ▶ ODBC 3.x syntax.
  - ▶ No change to the existing code.
  - ▶ Common SafeJDBC nucleus.
  - ▶ Windows NT 4 / 2000 / 2003.
  - ▶ Availability : Q2 2004.

# SafeJDBC for Oracle/OCI

- ▶ **SafeJDBC for Oracle/OCI:**
  - ▶ OCI: Oracle C++ Call Interface
  - ▶ OCI functions wrapper.
  - ▶ No JDBC driver required.
  - ▶ Unix/Linux.
  - ▶ Common SafeJDBC nucleus.
  - ▶ Windows NT4 / 2000 / 2003.
  - ▶ Availability : Q3 2004.

## Advantages of SafeJDBC

- ▶ SafeJDBC was designed to provide immediate data security while accommodating existing applications and production constraints.
- ▶ SafeJDBC deployment is fast, reliable, flexible, and economical.
- ▶ SafeJDBC allows transporting data risk-free between an application server and a DBMS server (without using SSL).
- ▶ SafeJDBC provides a central policy for maintaining data confidentiality in a multidatabase environment.

## Conclusion

**<http://www.safelogic.com>  
(<http://www.safejdbc.com>)**