

SafeJDBC

Chiffrement fort des données SQL Brief Technique

Nicolas de Pomereu – Directeur Associé

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

SafeJDBC - Driver JDBC de chiffrement fort

Plan :

- ▶ **Données SQL : constat & risques**
- ▶ **SQL : les solutions classiques de protection des données**
- ▶ **SafeJDBC - Objectifs**
- ▶ **Schémas de fonctionnement**
- ▶ **Technologie**
- ▶ **SafeJDBC pour Windows**
- ▶ **SafeJDBC pour Oracle**
- ▶ **Les avantages de SafeJDBC**

Données SQL : constat & risques encourus

Données SQL stratégiques & menaces:

▶ **Base clientèle**

- ▶ Contenus : coordonnées clients.
- ▶ Menaces : concurrents.

▶ **Base employés**

- ▶ Contenus : historiques, salaires, données privées ...
- ▶ Menaces : employés malveillants.

▶ **e-commerce**

- ▶ Contenus : numéros de CB, transactions.
- ▶ Menaces : pirates Internet.

SQL : les solutions classiques de protection

1. Les vendeurs SQL incluent des mesures de protection :

- ▶ Connexion par userid/password.
- ▶ Gestion de privilèges avec GRANT/REVOKE.
- ▶ Lien SSL entre l'application et la database.

Ces mesures protègent les accès à la base, mais pas les fichiers qui contiennent les données et qui restent en clair :

- ▶ Attaque sur les contenus par Internet ou en réseau.
- ▶ Simple vol ou recopie des disques durs...

SQL : les solutions classiques de protection

2. Chiffrement de partition système :

- ▶ Chiffrer une partition de données sur le disque dur. Elle est protégée par une clé secrète.
- ▶ La partition est chiffrée à l'arrêt → Vol des données impossible à l'arrêt de la machine

MAIS...

- ▶ Les données SQL seront toujours accessible en clair « à chaud » :
 - ▶ Le risque de piratage par réseau ne disparaît pas.
 - ▶ Un attaquant qui a un accès physique au serveur peut recopier le contenu du disque dur en clair « à chaud ».

SQL : les solutions classiques de protection

3. Interface de cryptographie entre les données SQL et l'application :

- ▶ Solution fiable.
- ▶ Les données sensibles sont stockées chiffrées en permanence « à froid » et « à chaud » dans la database SQL.
- ▶ L'applicatif chiffre et déchiffre les données à la volée avec une clé.
- ▶ En cas d'intrusion réseau ou de vol de disque dur, le contenu est inexploitable.

Chiffrement applicatif des données SQL

Développer une interface de cryptographie entre les données SQL et l'application :

MAIS...

- ▶ Les développements applicatifs nécessitent des spécialistes en cryptographie.
- ▶ Ces développements sont complexes.
- ▶ Ils doivent s'intégrer dans les contraintes de production.

**Quelle solution répond
à ces lourds inconvénients ?**



Article 34

« Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. »

http://ameli.senat.fr/publication_pl/2001-2002/203.html

La CNIL

Commission
Nationale
de l'Informatique
et des Libertés

Article 47

« Le montant de la sanction pécuniaire prévue au I de l'article 45 est proportionné à la gravité des manquements commis et aux avantages tirés de ce manquement.

Lors du premier manquement, il ne peut excéder 150 000 €
En cas de manquement réitéré dans les cinq années à compter de la date à laquelle la sanction pécuniaire précédemment prononcée est devenue définitive, il ne peut excéder 300 000 € ou, s'agissant d'une entreprise, 5 % du chiffre d'affaires hors taxes du dernier exercice clos dans la limite de 300 000 € »

http://ameli.senat.fr/publication_pl/2001-2002/203.html

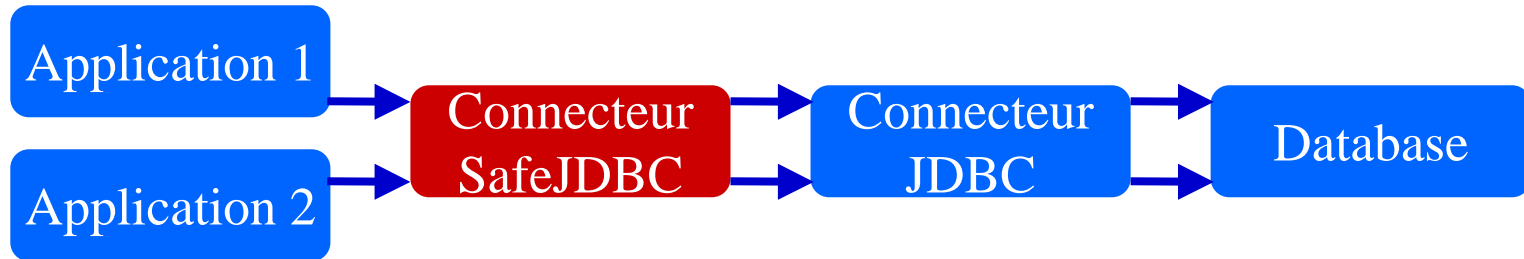
SafeJDBC - Objectifs

Trois objectifs principaux :

- 1. Protéger et sécuriser par chiffrement fort les contenus SQL « sensibles ».**
- 2. S'intégrer immédiatement dans les applicatifs Java sans ajout de code.**
- 3. S'intégrer dans la chaîne de production sans overhead sur le SGBD SQL.**

SafeJDBC

SafeJDBC intervient comme une couche supplémentaire standard dans l'architecture :



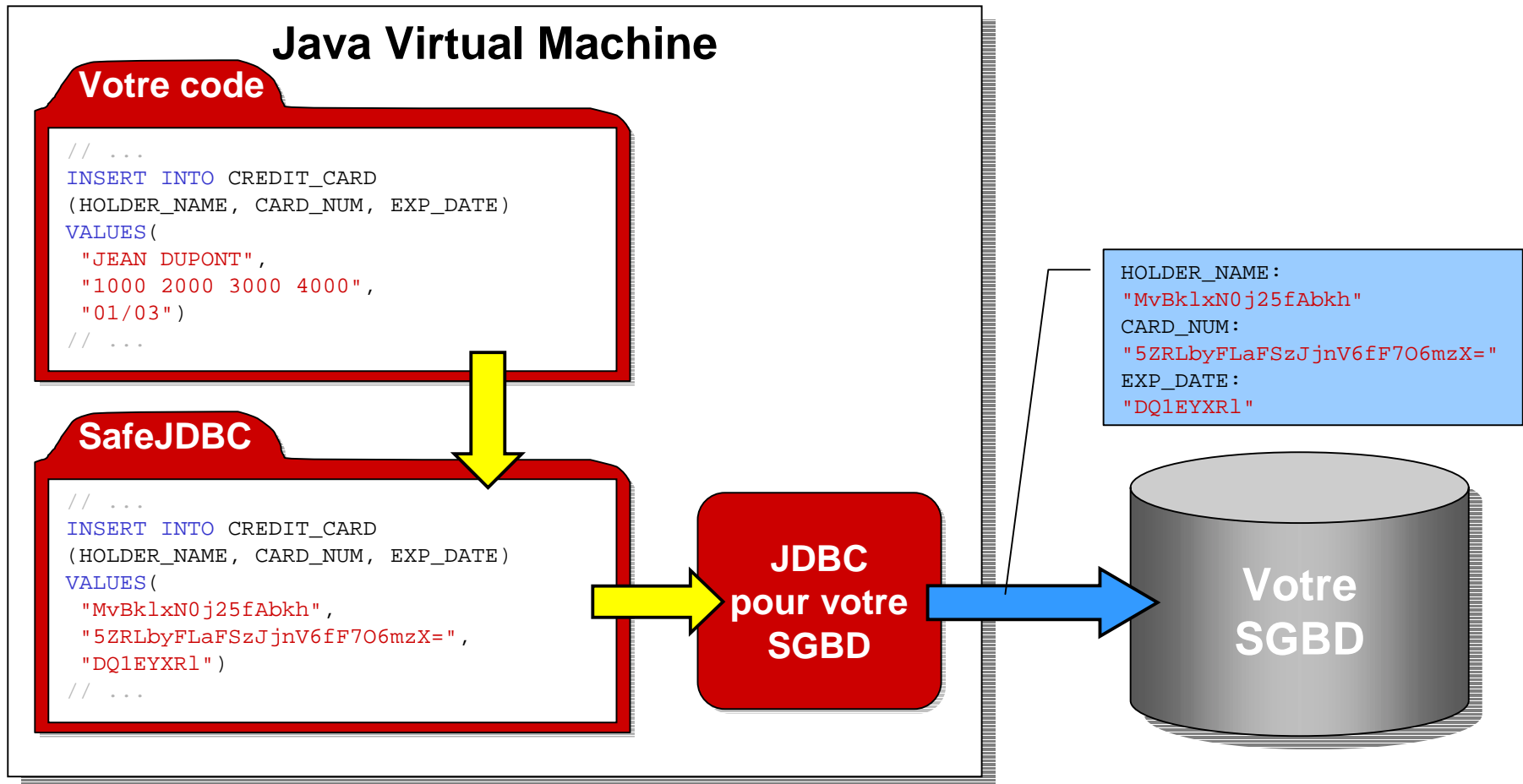
SafeJDBC interprète les requêtes pour protéger les données jugées sensibles par l'administrateur

<input checked="" type="checkbox"/>	Nom porteur
<input type="checkbox"/>	Numéro carte
<input type="checkbox"/>	Date expiration

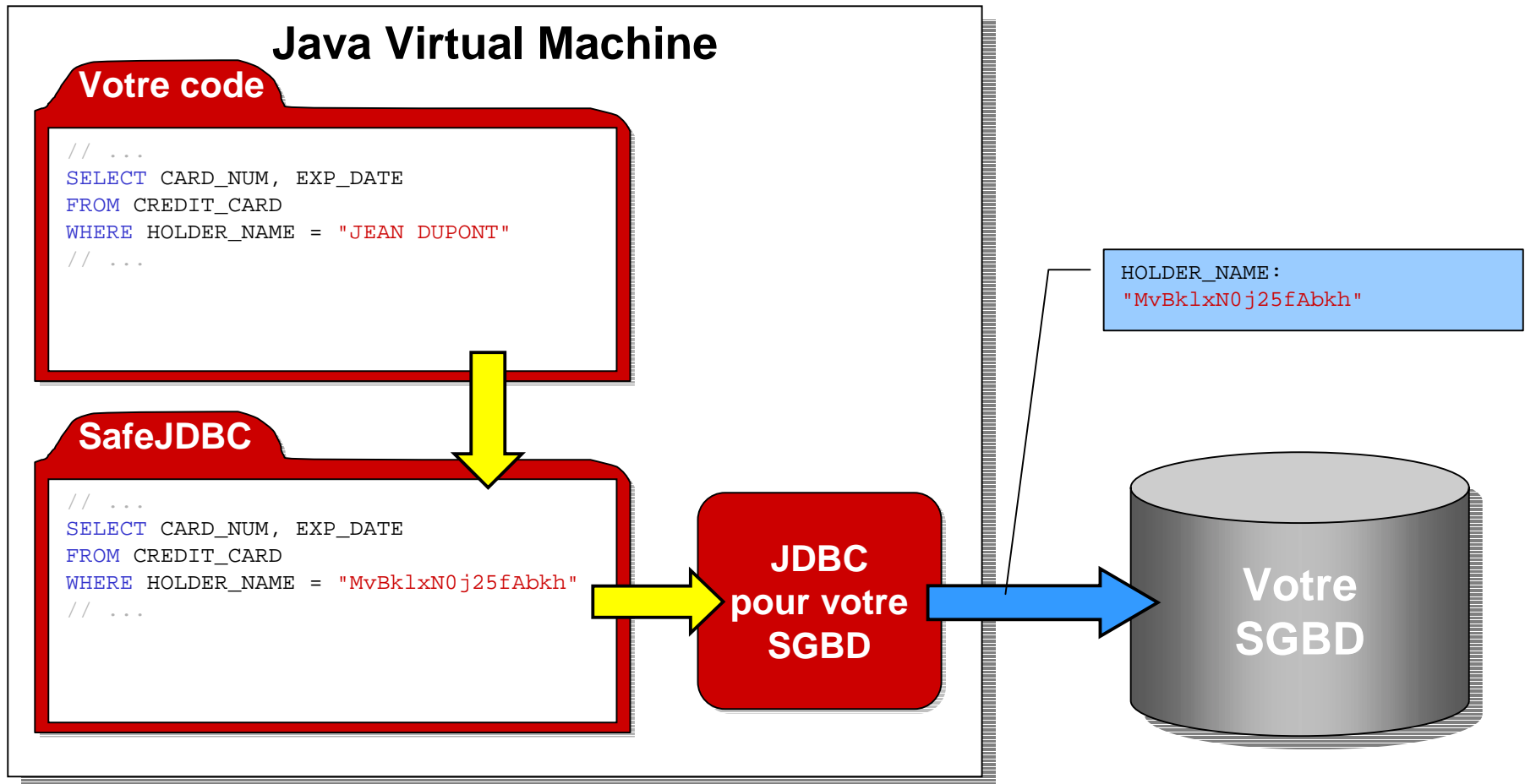
CREDIT_CARD_INFO

0452 6221 3578 4582

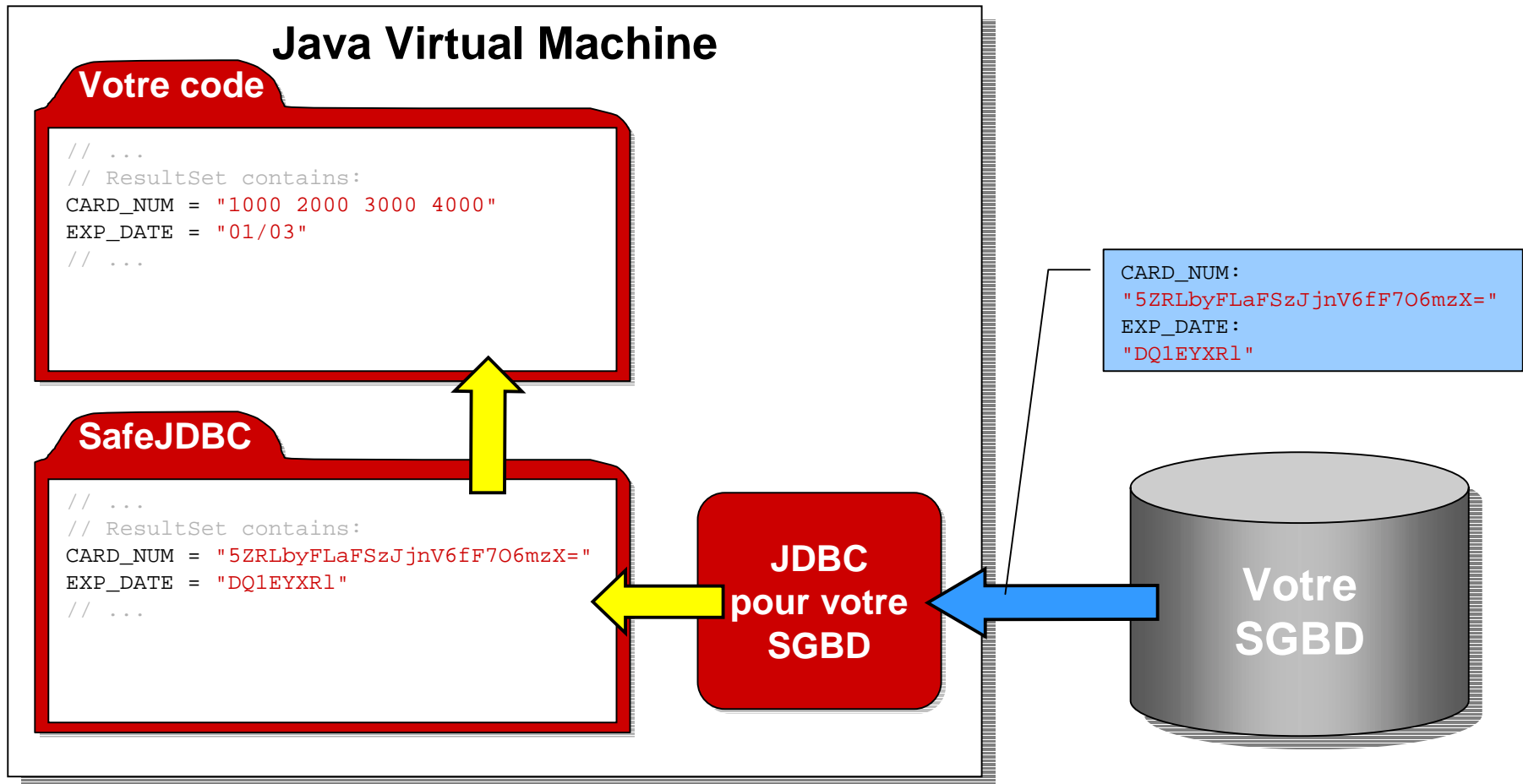
Insertion de données



Récupération de données : étape 1/2



Récupération de données : étape 2/2



Technologie

Principales caractéristiques :

- 1. Intégration plug-and-play dans le code Java existant sans nouveaux développements.**
- 2. Fonctionnement avec tous les SGBD SQL qui ont un driver JDBC 2.x ou 3.0.**
- 3. Fonctionnement avec les Application Server J2EE.**
- 4. Prise en compte des contraintes de production SQL (fiabilité et performances).**

Technologie

1. Intégration plug-and-play dans le code Java existant sans nouveaux développements :

- ▶ Aucune modification de code existant :
 - ▶ Tous les paramétrages se font via des fichiers de configuration. (Choix des colonnes à chiffrer).
 - ▶ Pas de recompilation du code Java.

- ▶ Garantie pour le déploiement :
 - ▶ Simplicité, souplesse, rapidité
 - ▶ Pas d'effets de bords & bugs.

Technologie

2. Fonctionnement avec tous les SGBD SQL qui ont un driver JDBC 2.x ou 3.0 :

- ▶ Compatibilité avec votre Driver JDBC :
 - ▶ SafeJDBC encapsule – en « passerelle » et sans overhead - les drivers JDBC existants.
 - ▶ Fonctionnement avec DB2, Informix, MySQL, Oracle, PostgreSQL, SQL Server, Sybase, ...
- ▶ Pérennité de l'investissement :
 - ▶ SafeJDBC s'intégrera avec les futurs drivers.

Technologie

1. Fonctionnement avec les Application Servers J2EE

- ▶ Intégration avec JNDI et DataSource (JDBC 3.0)
- ▶ Application Servers J2EE supportés :
 - ▶ BEA WebLogic,
 - ▶ IBM WebSphere,
 - ▶ JBoss,
 - ▶ Sun iPlanet,
 - ▶ Jakarta Tomcat.

Technologie

3. Prise en compte des contraintes de production SQL :

- ▶ **Aucun** accès au catalogue SQL.
- ▶ Les opérations de **chiffrement** sont effectuées uniquement dans **l'espace de la JVM** (Java Virtual Machine).
- ▶ Le stockage chiffré des données SQL n'entraîne **aucun trafic supplémentaire** entre la JVM et le moteur SQL.
- ▶ Overheads nuls ou très faibles sur les temps d'exécution du moteur SQL.

Technologie

▶ **Fact-sheet / Features :**

- ▶ Java 1.4 sous Windows NT/2000, Linux et Unix.
- ▶ Granularité du paramétrage des chiffrement au niveau de la table et colonne SQL.
- ▶ Compatible avec tout Driver JDBC 2.x et 3.0.
- ▶ Moteur de chiffrement extrait de SafeAPI agréé (DCSSI) et audité (Cryptolog)
- ▶ Chiffrement avec clés longues (128 bits).
- ▶ Choix des algorithmes :
 - ▶ Blowfish (CAST, IDEA en option).

Technologie

- ▶ **Fact-sheet / Features :**
 - ▶ Gestion transparente des clés secrètes :
 - ▶ Protection par passphrase (password long).
 - ▶ Possibilité de Clefs secrètes non stockées.
 - ▶ Formats gérés
 - ▶ INTEGER,
 - ▶ CHAR, VARCHAR, LONGVARCHAR,
 - ▶ BINARY, VARBINARY, LONGVARBINARY,
 - ▶ Large Objects : BLOB, CLOB.

Technologie

- ▶ **Fact-sheet / Features :**
 - ▶ Compatibilité SQL 2 :
 - ▶ Instructions normalisées DELETE, INSERT, SELECT, UPDATE.
 - ▶ Gestion des jointures sur colonnes SQL chiffrées.
 - ▶ API et interface de bascule pour applications existantes.
 - ▶ Gestion des retours arrière «en clair».
 - ▶ Si besoin : conseil & services SafeLogic.

SafeJDBC pour Windows (SafeODBC)

- ▶ **SafeJDBC pour Windows (SafeODBC):**
 - ▶ Driver ODBC.
 - ▶ Pur wrapper ODBC (DataSource).
 - ▶ Syntaxe ODBC 3.x.
 - ▶ Pas de modifications du code source.
 - ▶ Pas de recompilation des programmes.
 - ▶ Noyau commun SafeJDBC.
 - ▶ Windows NT 4 / 2000 / 2003.
 - ▶ Disponibilité : Q2 2004.

SafeJDBC pour Oracle/OCI

- ▶ **SafeJDBC pour Oracle/OCI :**
 - ▶ OCI: Oracle C++ Call Interface
 - ▶ Wrapper des fonctions OCI.
 - ▶ Ne nécessite pas de Driver JDBC.
 - ▶ Unix/Linux.
 - ▶ Noyau commun SafeJDBC.
 - ▶ Windows NT4 / 2000 / 2003.
 - ▶ Disponibilité : à définir.

Les avantages de SafeJDBC

- ▶ SafeJDBC a été conçu pour sécuriser immédiatement les données en tenant compte de l'existant applicatif et des contraintes de production.
- ▶ SafeJDBC offre une mise en œuvre fiable, souple, économique et très rapide.
- ▶ SafeJDBC permet de véhiculer sans risque les données entre un Serveur d'Application et un serveur SGBD (sans utiliser de SSL).
- ▶ SafeJDBC permet de centraliser la politique de confidentialité des données dans un environnement multi-bases.

Conclusion

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