
ORACLE®

MySQL Enterprise Edition Security - Transparent Data Encryption

Mike Frank / マイク フランク
MySQL Global Business Unit
Product Management Director

Safe Harbor Statement

以下の事項は、弊社の一般的な製品の方向性に関する概要を説明するものです。
また、情報提供を唯一の目的とするものであり、いかなる契約にも組み込むことはできません。
以下の事項は、マテリアルやコード、機能を提供することをコミットメントするものではない為、購買決定を行う際の判断材料になさらないで下さい。

オラクル製品に関して記載されている機能の開発、リリースおよび時期については、弊社の裁量により決定されます。

大規模な不正アクセス

2013年には5億レコード以上の個人情報が流出。レコード数は1年で5倍増

77%

Webサイトの脆弱性
さらに8件に1件は
深刻な脆弱性

8

2013年に1,000万レコード以上の被害に遭った不正アクセス事件

2013年の不正アクセス件数は62%増

Source: Internet Security Threat Report 2014, Symantec

ORACLE

Regulatory Drivers

- Regulations
  - PCI – DSS: Payment Card Data
  - HIPAA: Privacy of Health Data
  - Sarbanes Oxley: Accuracy of Financial Data
  - EU Data Protection Directive: Protection of Personal Data
  - Data Protection Act (UK): Protection of Personal Data
- Requirements
  - Continuous Monitoring (Users, Schema, Backups, etc)
  - Data Protection (Encryption, Privilege Management, etc.)
  - Data Retention (Backups, User Activity, etc.)
  - Data Auditing (User activity, etc.)

PCI Security Standards Council

HIPAA
Health Insurance Portability and Accountability Act

Sarbanes-Oxley
Financial and Accounting Disclosure Information

European Commission
Justice

Data Protection Act 1998

PCI DSS

PCI DSS v3.0
November 2013

3.5 Store cryptographic keys in a secure form (3.5.2), in the fewest possible locations (3.5.3) and with access restricted to the fewest possible custodians (3.5.1)

3.6 Verify that key-management procedures are implemented for periodic key changes (3.6.4)

And more!

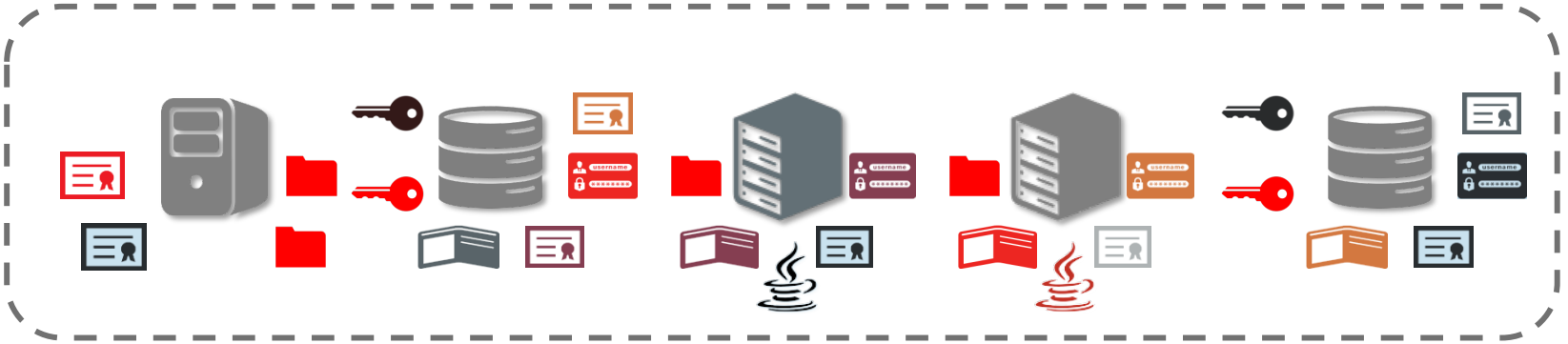
MySQL Enterprise Edition

- New! MySQL Enterprise TDE
  - Data-at-Rest Encryption
  - Key Management/Security
- MySQL Enterprise Authentication
  - External Authentication Modules
    - Microsoft AD, Linux PAMs
- MySQL Enterprise Encryption
  - Public/Private Key Cryptography
  - Asymmetric Encryption
  - Digital Signatures, Data Validation
  - User Activity Auditing, Regulatory Compliance
- MySQL Enterprise Firewall
  - Block SQL Injection Attacks
  - Intrusion Detection
- MySQL Enterprise Audit
  - User Activity Auditing, Regulatory Compliance
- MySQL Enterprise Monitor
  - Changes in Database Configurations, Users Permissions, Database Schema, Passwords
- MySQL Enterprise Backup
  - Securing Backups, AES 256 encryption

What is Transparent Data Encryption?

- Data at Rest Encryption
  - Tablespaces, Disks, Storage, OS File system
- Transparent to applications and users
  - No application code, schema or data type changes
- Transparent to DBAs
  - Keys are hidden from DBAs, no configuration changes
- Requires Key Management
  - Protection, rotation, storage, recovery

Biggest Challenge: Encryption Key Management



Management

- Proliferation of encryption wallets and keys
- Authorized sharing of keys
- Key availability, retention, and recovery
- Custody of keys and key storage files

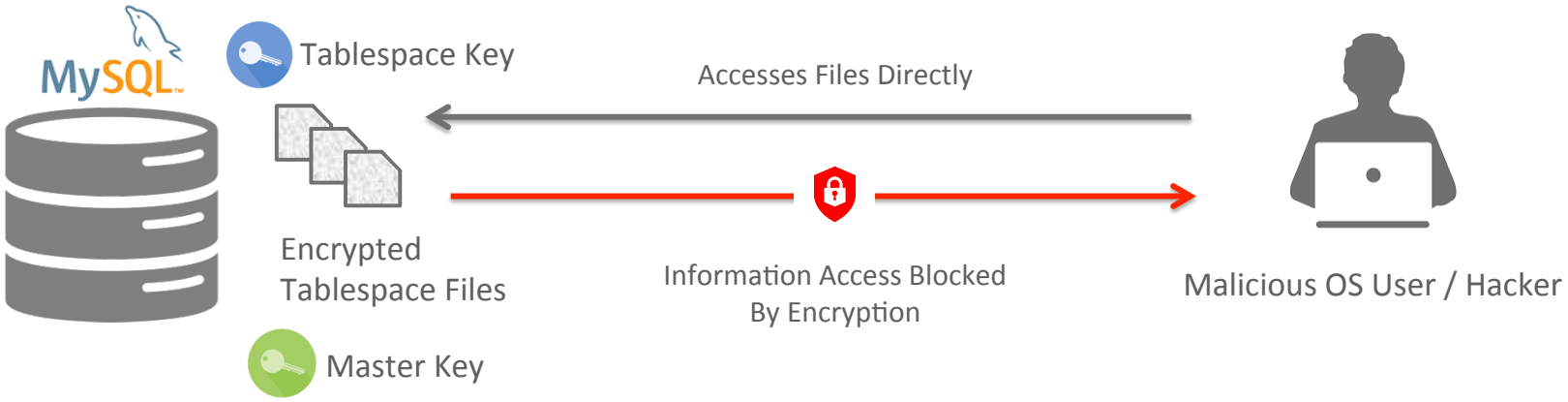
Regulations

- Physical separation of keys from encrypted data
- Periodic key rotations
- Monitoring and auditing of keys
- Long-term retention of keys and encrypted data

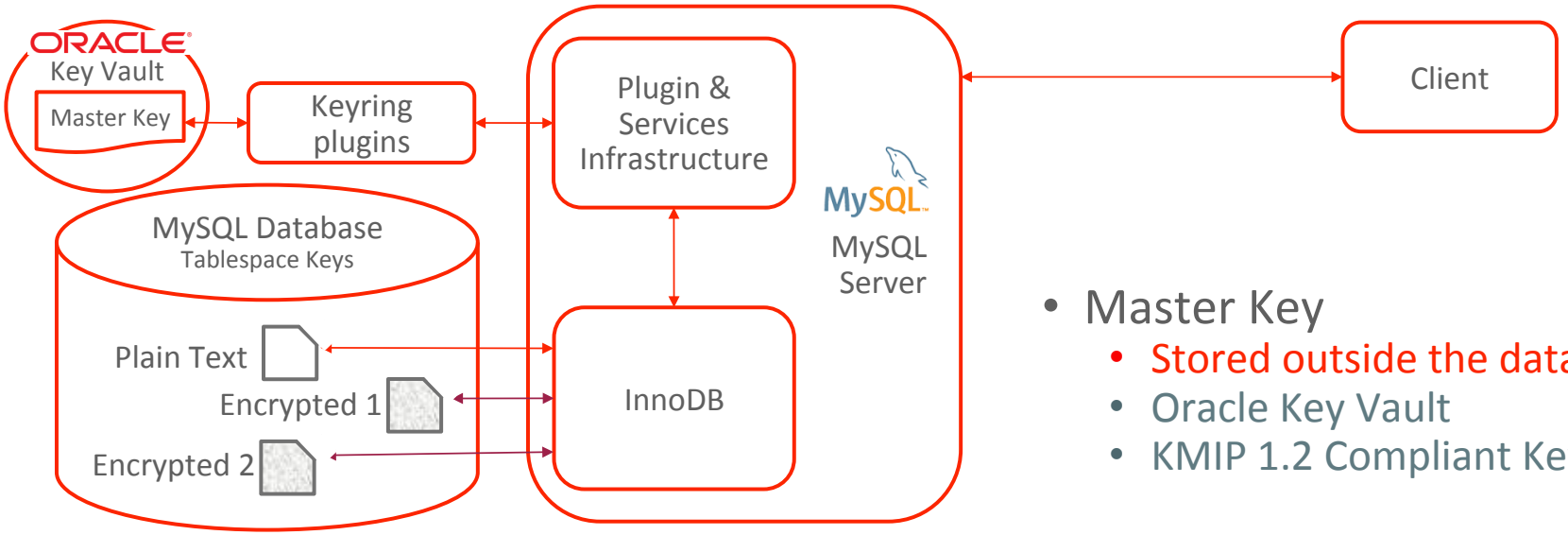
MySQL Enterprise TDE: Goals

- Data at Rest Encryption
  - Tablespace Encryption
- Key Protection
  - Most Important and Difficult
- Strong Encryption
  - AES 256
- Simple to Manage
  - One master key for whole MySQL instance
- High Performance & Low Overhead
  - Simple Key Rotation without massive decrypt/encryption costs
- High Quality Infrastructure
  - Expand and support more security capabilities - encryption, keys, certs, …

MySQL Transparent Data Encryption

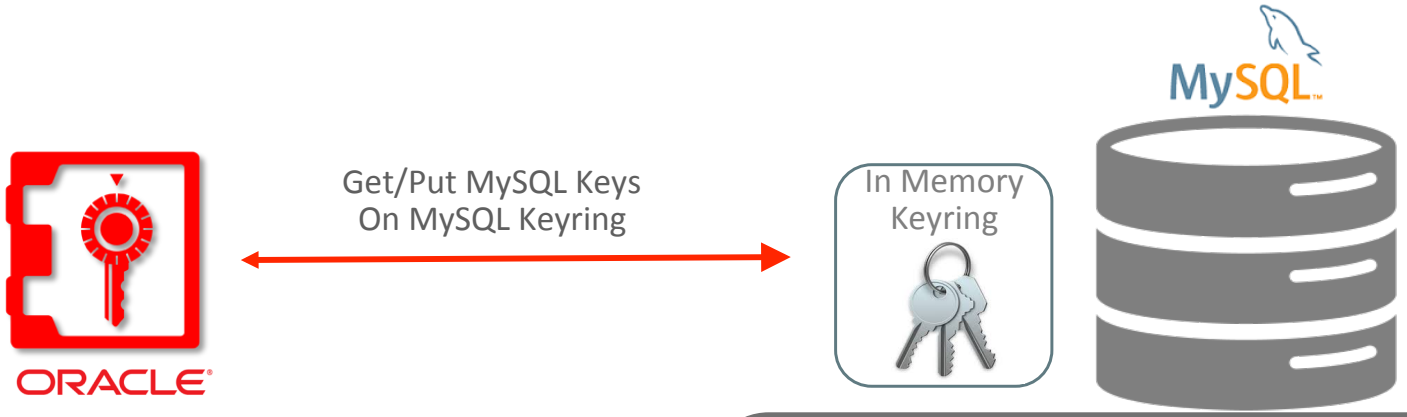


MySQL Transparent Data Encryption: 2 Tier Architecture



- Master Key
  - Stored outside the database
  - Oracle Key Vault
  - KMIP 1.2 Compliant Key Vault
- Tablesapce Key
  - Protected by master key

MySQL Key Ring



Key Vault
or KMIP v1.2 Compliant Key Vault

- Keys are only accessible to internal components
  - Internal Code or Internal plugins
- Key Rings are not persistent
  - In memory and protected in memory
- ACLs for who key is for
  - i.e. InnoDB Tablespaces

ORACLE

Using MySQL Transparent Data Encryption

SQL

- New option in CREATE TABLE ENCRYPTION="Y"
- New SQL : ALTER INSTANCE ROTATE INNODB MASTER KEY

Plugin Infrastructure

- New plugin type : keyring
- Ability to load plugin before InnoDB initialization : --early-plugin-load

Keyring plugin

- Used to retrieve keys

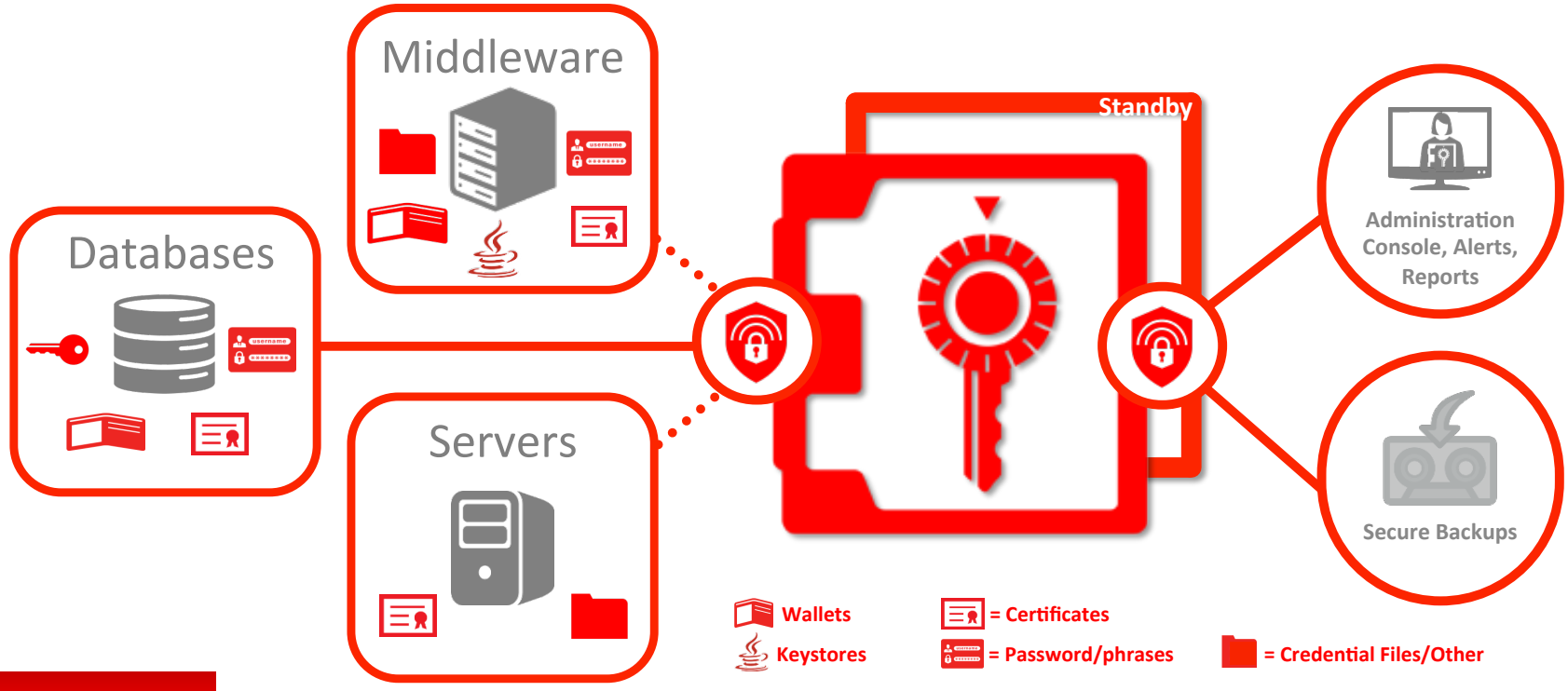
InnoDB

- Support for encrypted tables
- IMPORT/EXPORT of encrypted tables
- Support for master key rotation

Encryption Key Management

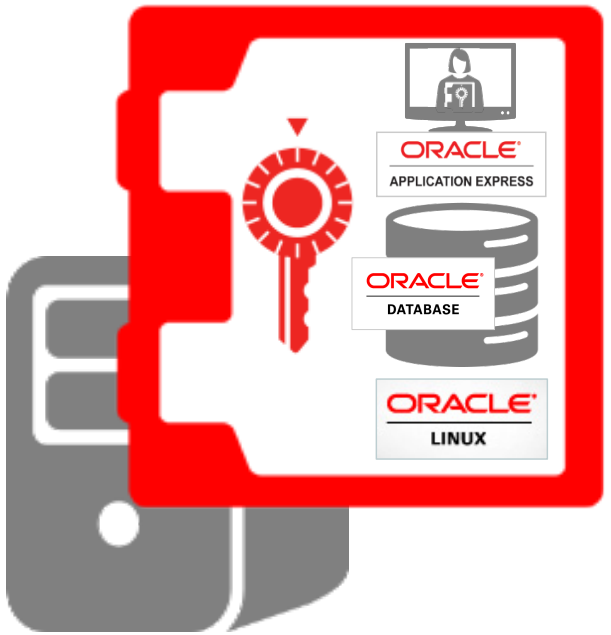
Key Vaults and Key Stores

Key Vaults and Key Stores: General Purpose



Oracle Key Vault

- Turnkey solution based on hardened stack
- Includes Oracle Database and security options
- Open x86-64 hardware to choose from
- Easy to install, configure, deploy, and patch
- Separation of duties for administrative users
- Full auditing, preconfigured reports, and alerts



MySQL Enterprise TDE: Oracle Key Vault KMIP Compliant

- Uses Oracle KMIP Client Library
- DBA never knows the Master Key
- Only a Oracle Key Vault Admin(s) have Master Key access
- Keys are protected and secure
- Oracle Key Vault has built-in redundancy, backup
- Enables customers to meet regulatory requirements

Example Commands

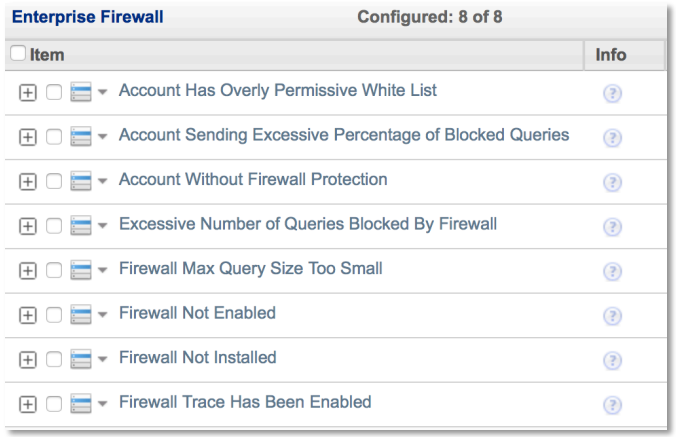
- Installation
  - Set configuration for MySQL to talk to Oracle Key Vault
  - Connect to MySQL
    - `install plugin okv_kmip_keyring_file soname 'okv_kmip_keyring.dll';`
- Encrypt a table
  - ```
    CREATE TABLE `<table>` (  `ID` int(11) NOT NULL
    AUTO_INCREMENT,   `Name` char(35) NOT NULL DEFAULT '',
    … ) ENGINE=InnoDB … ENCRYPTION="Y"
    ```
- Rotate Master Key
  - `ALTER INSTANCE ROTATE INNODB MASTER KEY;`
    ```

Notes about configuration

- --early-plugin-load
  - Usage : same as –plugin-load : “<plugin>=<library>”
  - Loading keyring plugin from Oracle Key Vault into the instance before InnoDB starts:
  - Enables recovery of encrypted tablespaces

MySQL Enterprise Firewall

- SQLインジェクション対策、リアルタイム保護
  - ホワイトリストモデル、
    実行されるクエリーを分析しホワイトリストと照合
- 学習してホワイトリストを自動作成
  - ユーザー毎に、SQL実行パターンを記録して
    自動的にホワイトリストを作成
- 不審なアクセスを「検知」または「ブロック」
  - ポリシーに違反するトランザクションを「検知」しログに記録
  - ポリシーに違反するトランザクションを「検知」しログに記録しつつ、「ブロック」
- 透過的
  - アプリケーションを変更する必要無し



MySQL Enterprise Firewall monitoring

MySQL Enterprise Authentication
外部認証のサポート

Integrates MySQL with existing security infrastructures

- PAM（Pluggable Authentication Modules）
  - 外部認証方式へのアクセス
  - 標準のインタフェース（Unix, LDAP, Kerberosなど）
  - プロキシ／非プロキシユーザー
- Windows
  - ネイティブWindowsサービス（WAD）へのアクセス
  - Windowsにログイン済みユーザを認証
- プラガブル認証API

MySQLアプリケーションを既存のセキュリティ・インフラストラクチャ/SOPと統合

ORACLE

MySQL Enterprise Encryption

非対称暗号: RSA, DSA, and DH 等の暗号化をサポート

- MySQLの暗号化ライブラリ
  - AES256による対称鍵暗号
  - 公開鍵 / 非対称鍵暗号
- キーの管理
  - 公開鍵および秘密鍵の生成
  - 鍵交換方式: RSA, DSA, DH
- 署名とデータの検証
  - 電子署名、検証、妥当性確認のための暗号学的ハッシュ関数

ORACLE

MySQL Enterprise Audit

ポリシーベースの監査機能を提供

Adds regulatory compliance to MySQL applications (HIPAA, Sarbanes-Oxley, PCI, etc.)

- ログオン、クエリーの情報を監査可能
- ユーザがポリシーを設定可能：フィルタリング、ログローテーション
- 動的に設定を変更可能：Audit設定時にサーバの再起動が不要
- Oracleの仕様に合わせXMLベースの監査ログを出力
  （Oracle Audit Vaultとの互換性（ログフォーマット））
- サイズに基づいた監査ログファイルの自動ローテーション
- MySQL 5.5のAudit APIを使って実装 / MySQL 5.5.28 以上で使用可能

コンプライアンス対応等で監査が必要なアプリケーションでもMySQLを利用可能

ORACLE

Integrated Cloud

Applications & Platform Services


ORACLE®