HSMを利用したデータベース暗号化

タレスジャパン株式会社

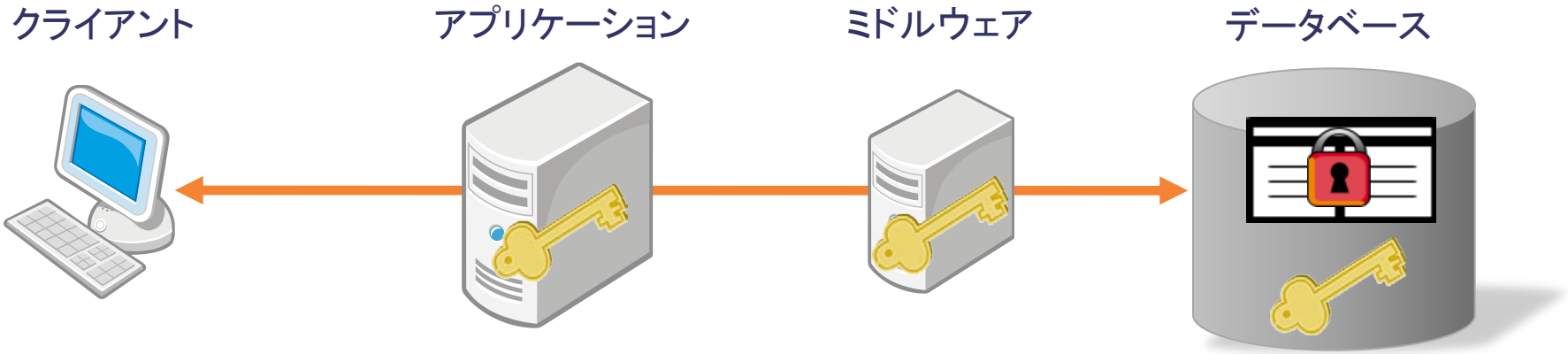
2011年7月26日　JCDSCベンダー部会

www.thalesgroup.com/japan

THALES

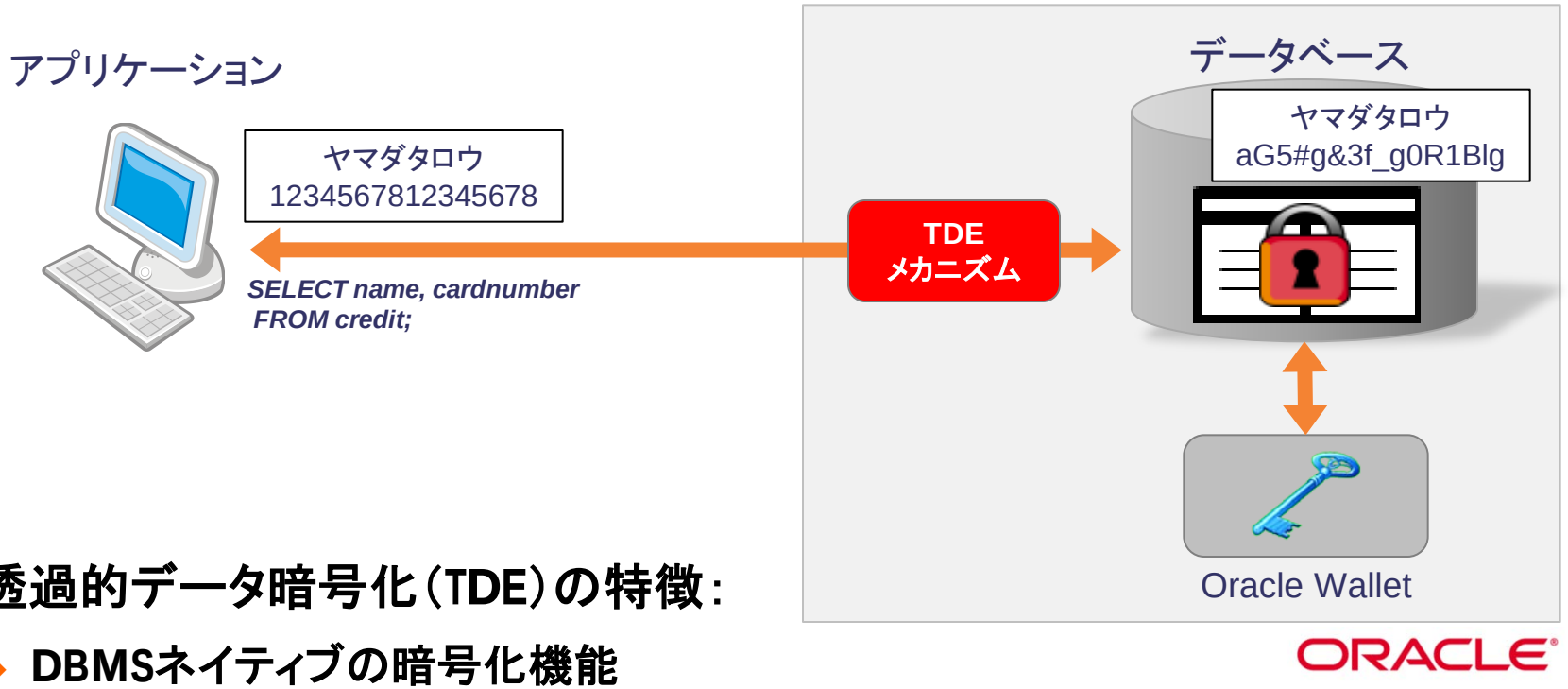
データベース暗号化

- 暗号化を実施するポイントによって数種類の方式



- データベース暗号化に対する懸念
  - 暗号処理のオーバヘッドでパフォーマンスの低下が心配…
  - アプリケーションの改修が必要…
  - システムの構成が複雑になって運用の負荷が増大…
  - 暗号化したデータを戻せなくなったら…
- データベースの透過的データ暗号化機能 (TDE) は、これらの懸念に対する有力なソリューション

透過的データ暗号化 (TDE)



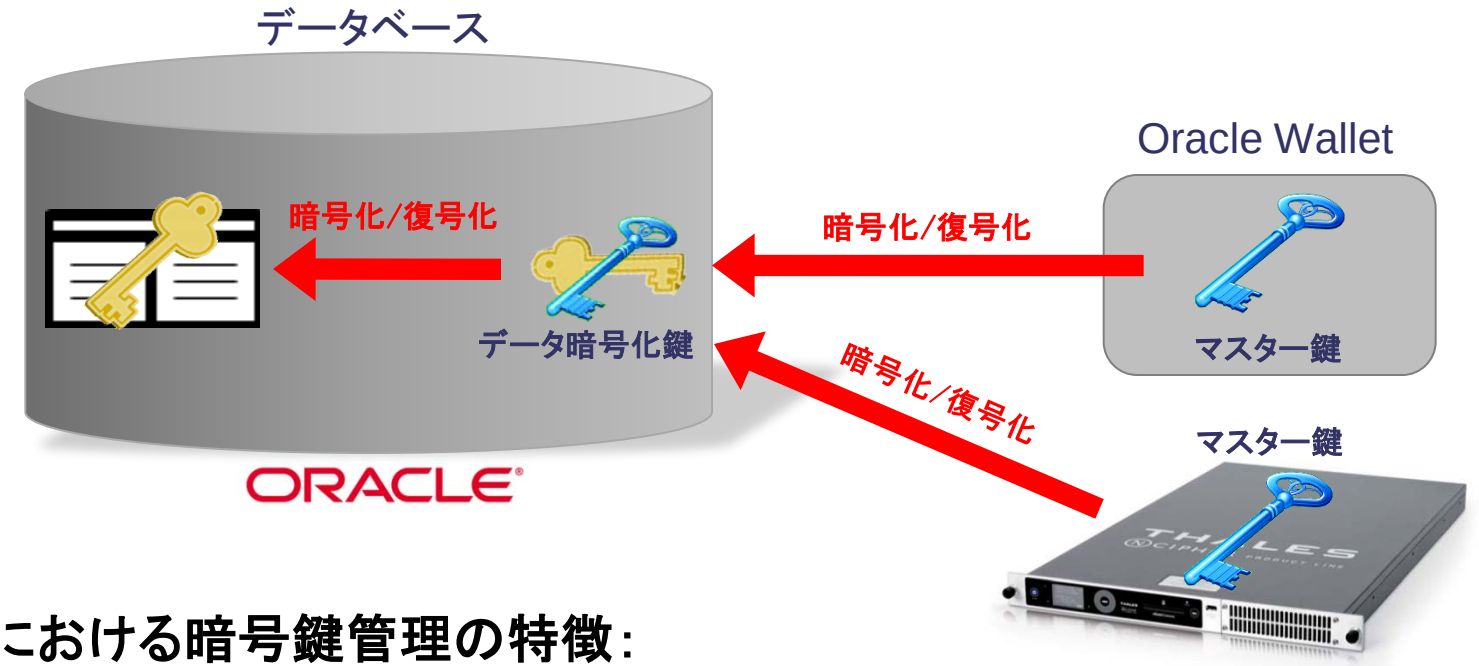
透過的データ暗号化（TDE）の特徴：

- **DBMSネイティブの暗号化機能**
- **アプリケーションからは透過的に、データの暗号化/復号化が行われる**
  - 既存のアプリケーション（SQL）を改修する必要はない
- **AES(128/192/256bit) に対応**
- **Oracle Wallet を利用した鍵管理メカニズム**

ORACLE

THALES

TDE における暗号鍵管理



TDE における暗号鍵管理の特徴：

- マスター鍵とデータ暗号鍵による2重のセキュリティ
  - データベース内のデータを「データ暗号化鍵」で暗号化
  - データ暗号化鍵を「マスター鍵」で暗号化
- Oracle Walletはデータベースサーバ上の”ファイル”であり、パスワードによる保護のみ
- 効果的な暗号鍵管理のために、安全なマスター鍵の格納庫としてHSMを標準サポート

THALES

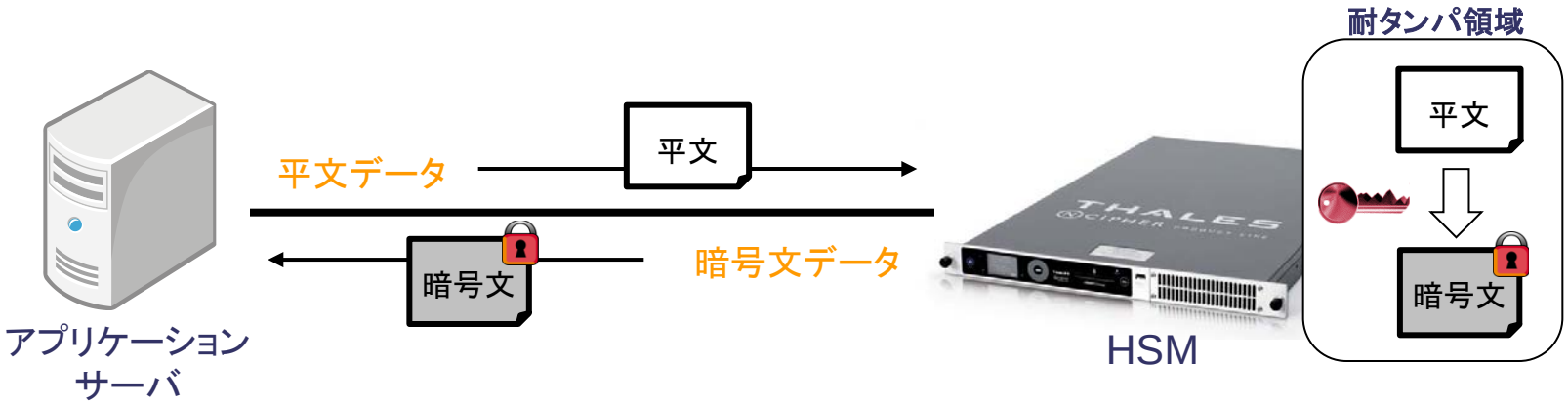
Thales nShield HSM (Hardware Security Module)

暗号鍵を保護する専用のハードウェア

暗号処理をHSM内部で安全かつ高速に実行

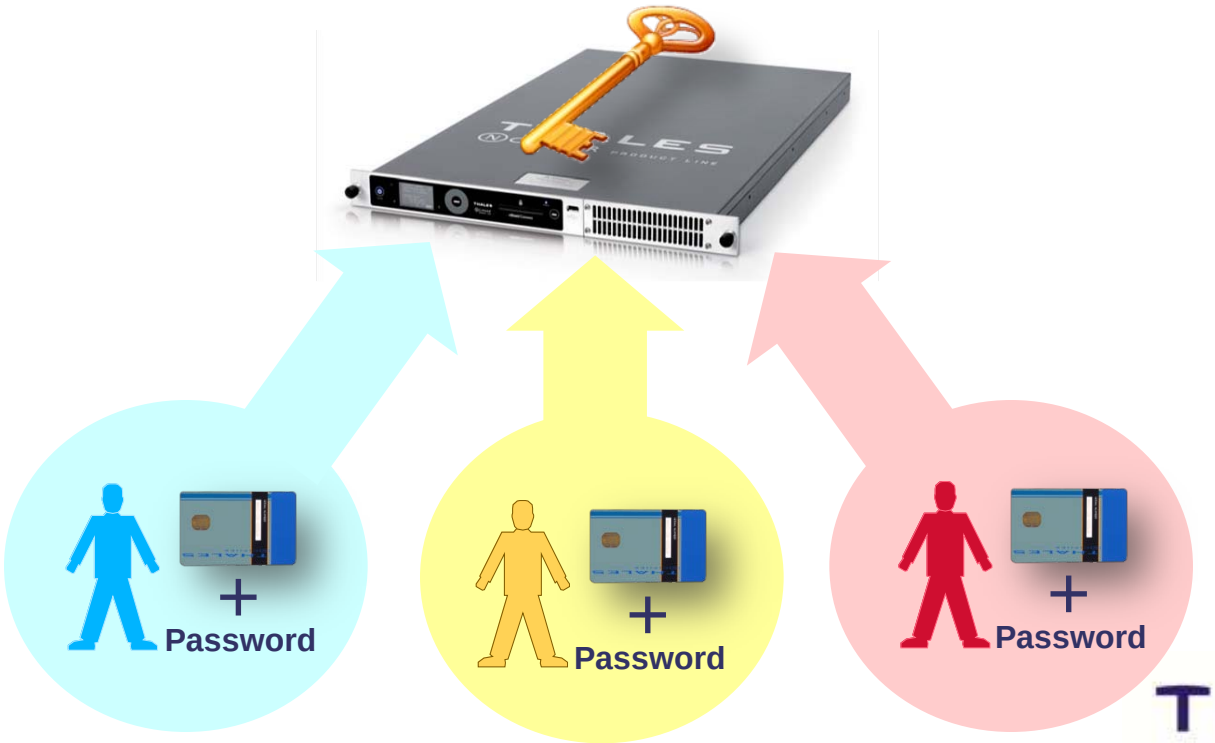
強力な暗号鍵へのアクセスコントロール（2要素認証）

物理的な不正アクセスから暗号鍵を防御（耐タンパ機能）



HSMによるPCIDSS要件の達成

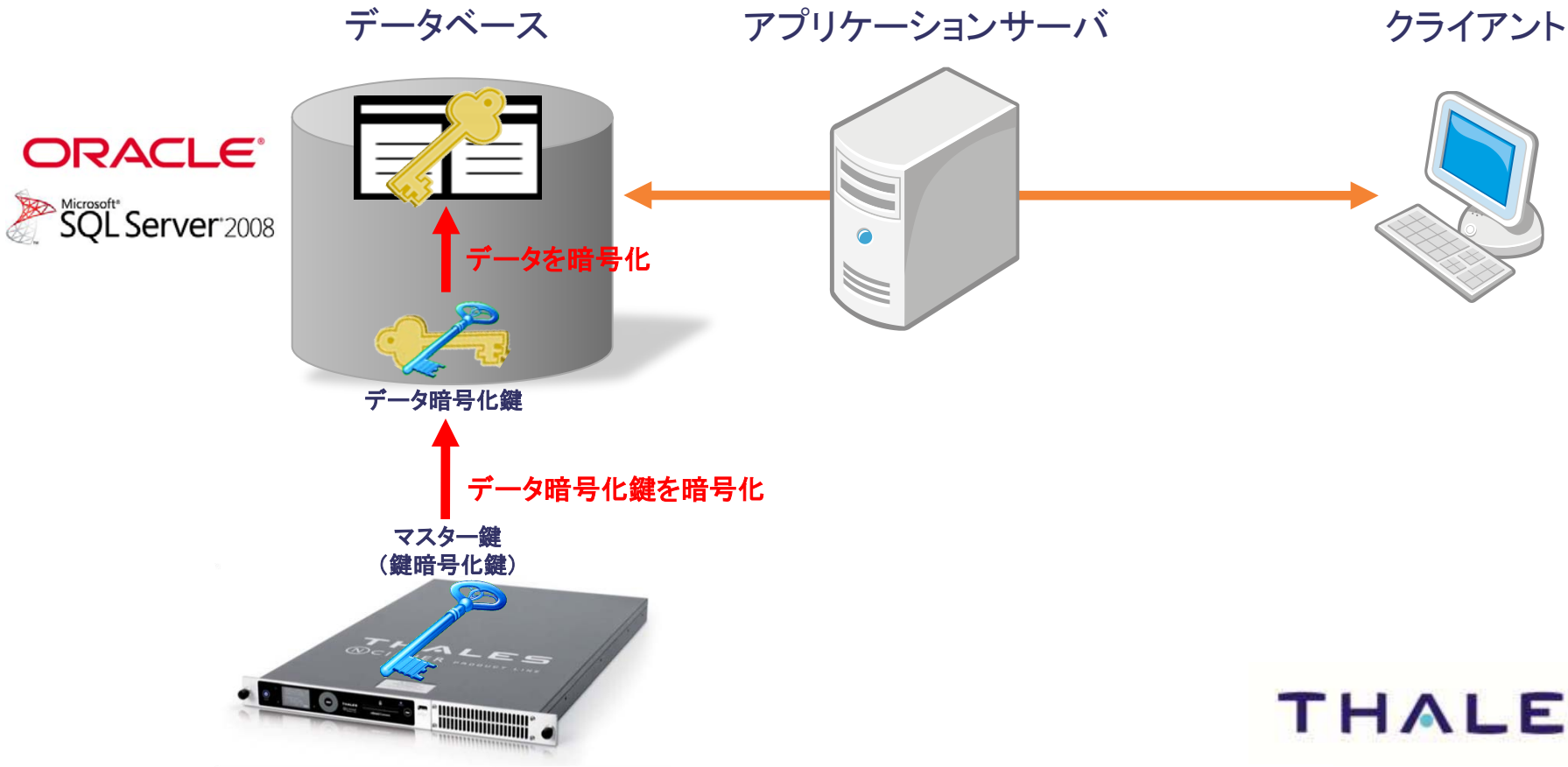
- **3.5 暗号化キーを開示や誤使用から保護する**
  - 3.5.1 暗号化キーへのアクセスを、必要最小限の管理者に制限する
- **3.6 暗号化キーの管理プロセスおよび手順を文書化し実装する**
  - 3.6.6 暗号化キーの知識分割と二重管理
  - 3.6.7 暗号化キーの不正置換の防止



THALES

HSMによるPCIDSS要件の達成

- **3.5 暗号化キーを開示や誤使用から保護する**
  - 3.5.2 暗号化キーの保存場所と形式を最小限にし、安全に保存する
    - **3.5.2.a キーが暗号化された形式で保存され、キー暗号化キーがデータ暗号化キーとは別個に保存されていること**



THALES

HSMによるPCIDSS要件の達成

- **3.6 暗号化キーの管理プロセスおよび手順を文書化し実装する**
  - 3.6.1 強力な暗号化キーの生成
  - 3.6.2 安全な暗号化キーの配布
  - 3.6.3 安全な暗号化キーの保存

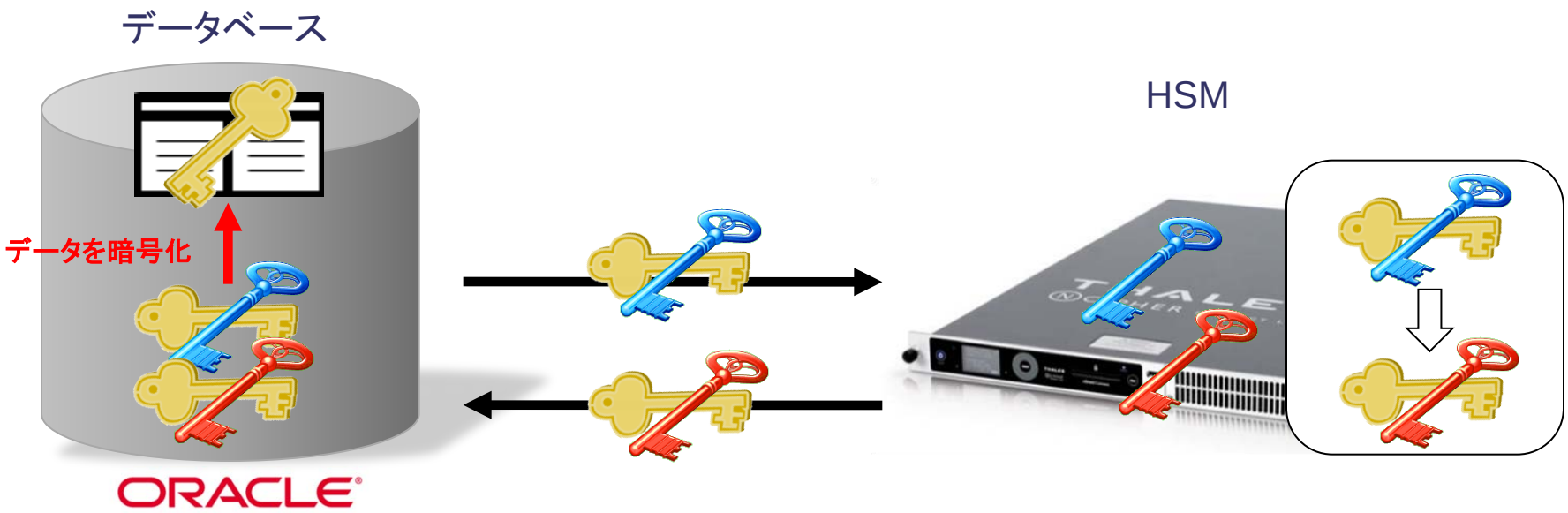
FIPS VALIDATED 140-2

Common Criteria

THALES

HSMによるPCIDSS要件の達成

- **3.6 暗号化キーの管理プロセスおよび手順を文書化し実装する**
  - 3.6.4 定期的な暗号化キーの変更



SQL> ALTER SYSTEM SET ENCRYPTION KEY ...

THALES

まとめ

- **データベースとのシームレスな連携**
  - データベースのネイティブな暗号化機能に、強力な暗号鍵の保護を追加
  - DBMSのオプション機能として、業界標準のPKCS#11 API経由で連携
- **保証されたセキュリティ**
  - FIPS140-2 Level3、Common Criteria EAL4+ 認証を取得
  - ハードウェアベースの鍵の保護
  - 高度な役割分割、強力なユーザー認証
- **コンプライアンス要件への準拠を支援**
  - PCIDSS 要件3の暗号鍵管理要件を効果的に実現

お問い合わせ先

- 製品情報

  http://www.thales-esecurity.com/japan

- 製品購入に関するお問い合わせ:

  タレスジャパン株式会社

  代表: 03-5785-1975

  Jpnsales@thales-esecurity.com

THALES