THALES

鍵管理の標準化動向と必要性

Jiro Shindo
Product Manager
Thales Information System Security

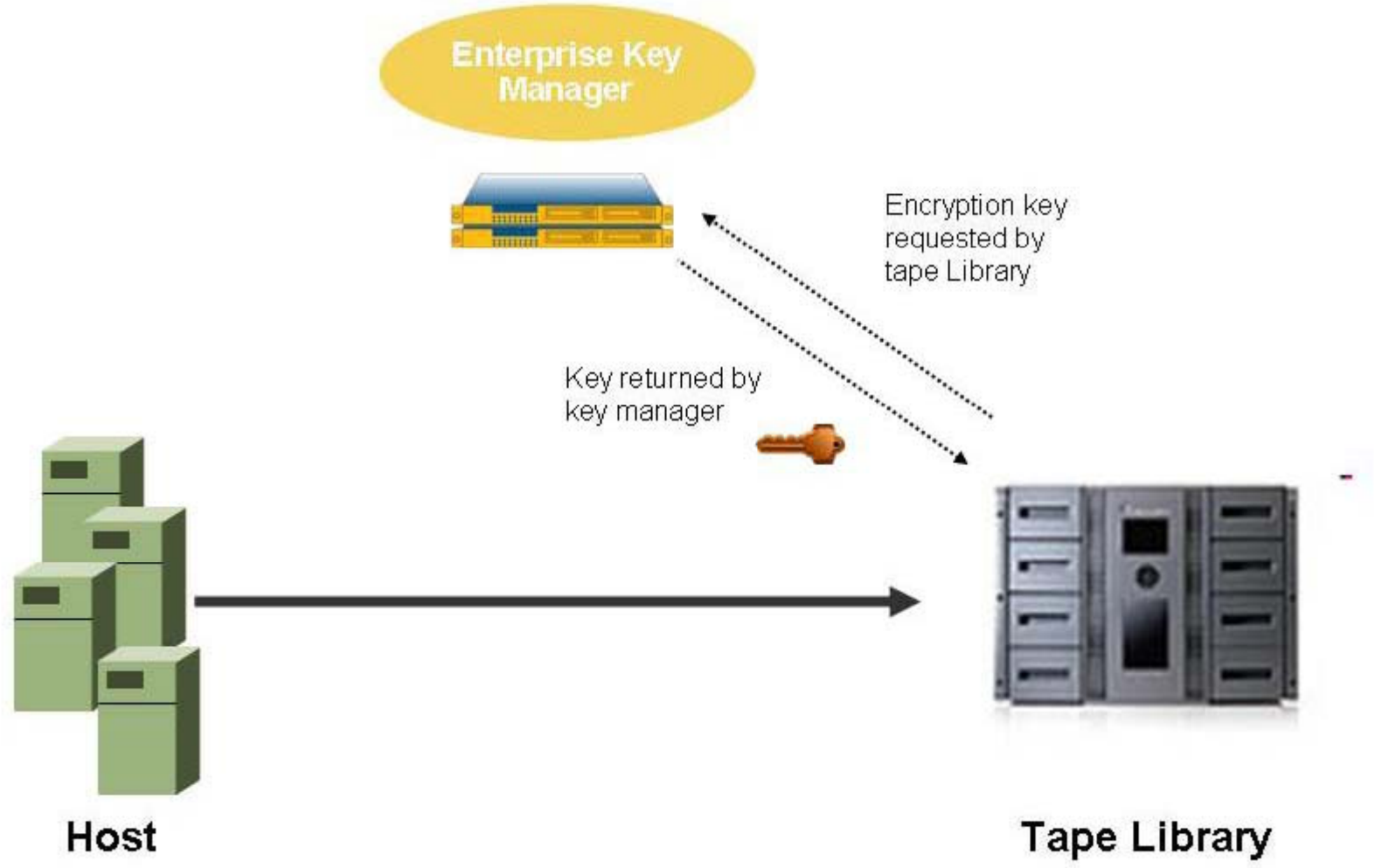
Agenda

- 鍵管理における相互運用の必要性
- KMIP 概要
- KMIP 仕様
- OASIS KMIP 技術委員会
- 集中型鍵管理の事例

The Need for Interoperable Key Management

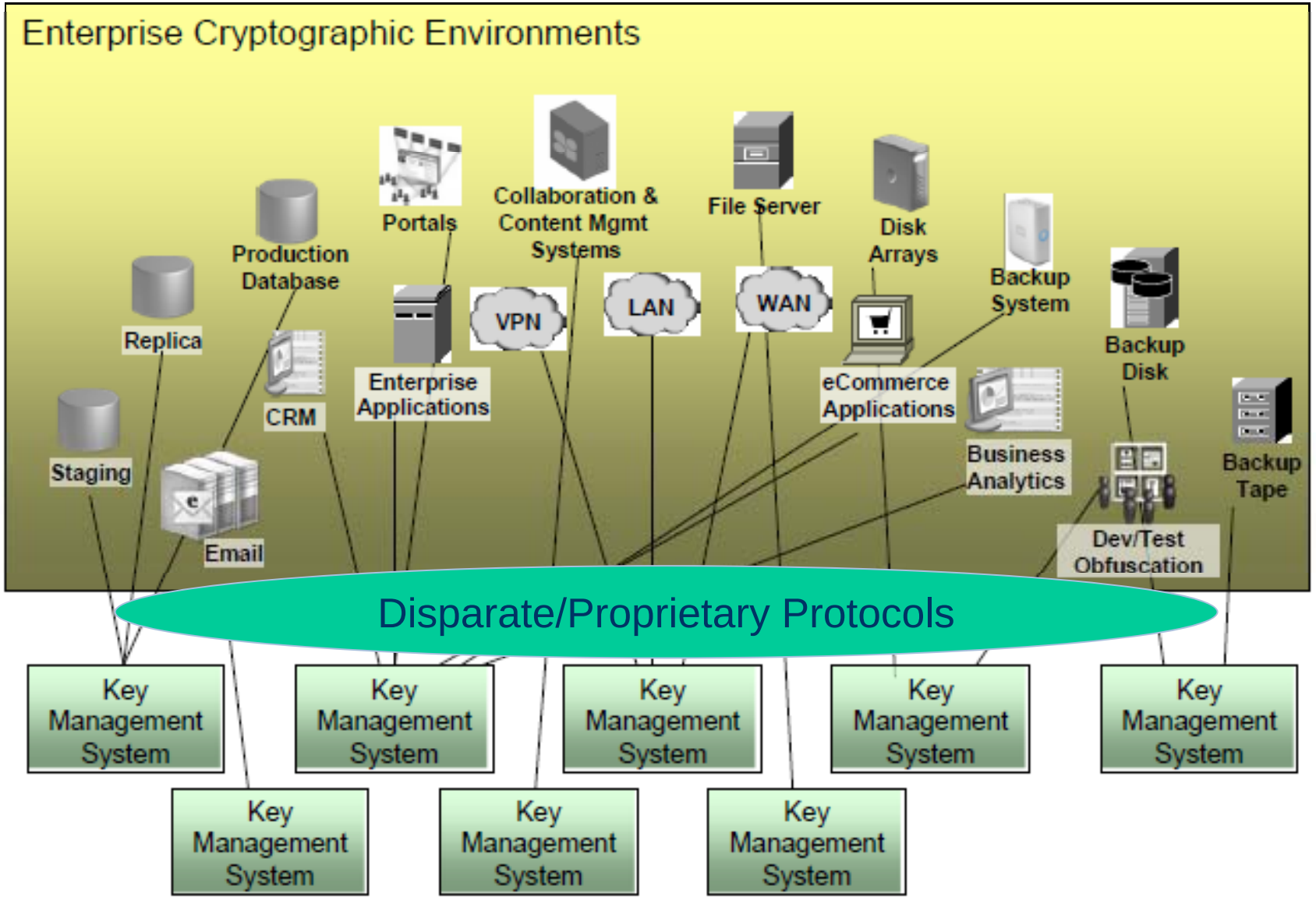
- 今日の企業はより複雑なマルチベンダ環境で運用している
- 企業内を横断する暗号化を展開する必要がある
- “暗号化したデータを回復できる事” がIT管理者が暗号化を展開する上での大きな課題である
- 今日多くの企業が用途毎に別々の暗号化システムを展開している
  – PC, ストレージ, データベース, アプリケーション – その結果:
  - 煩雑性、暗号鍵を管理するためにしばしば手動の処理が必要
  - ITコストの増加
  - セキュリティ標準と監査の条件を達成するための課題
  - データの消失

Encryption and Key Management



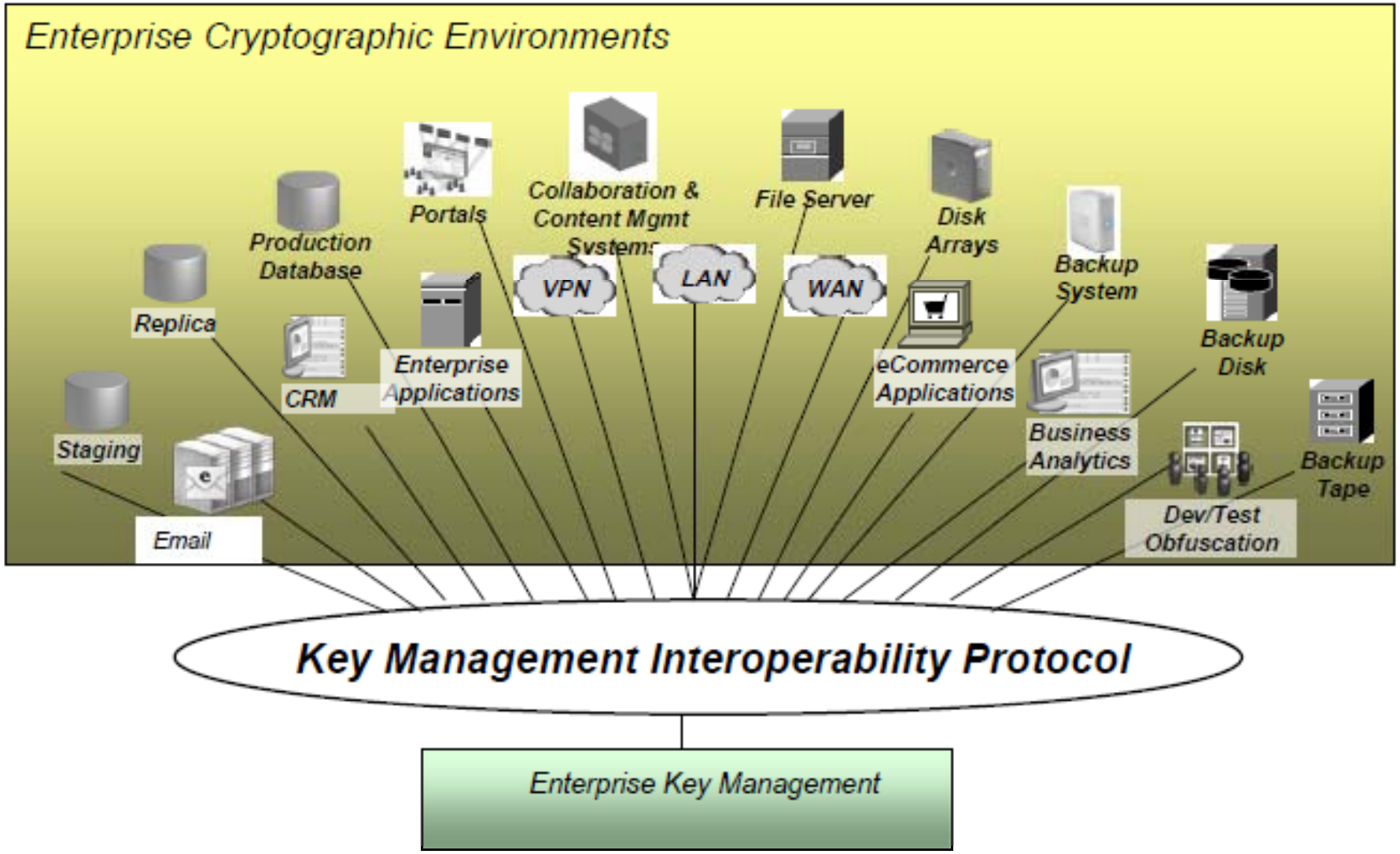
THALES

Today: Each Cryptographic Environment Has Its Own Key Management System



THALES

KMIP: Single Protocol Supporting Enterprise Cryptographic Environments



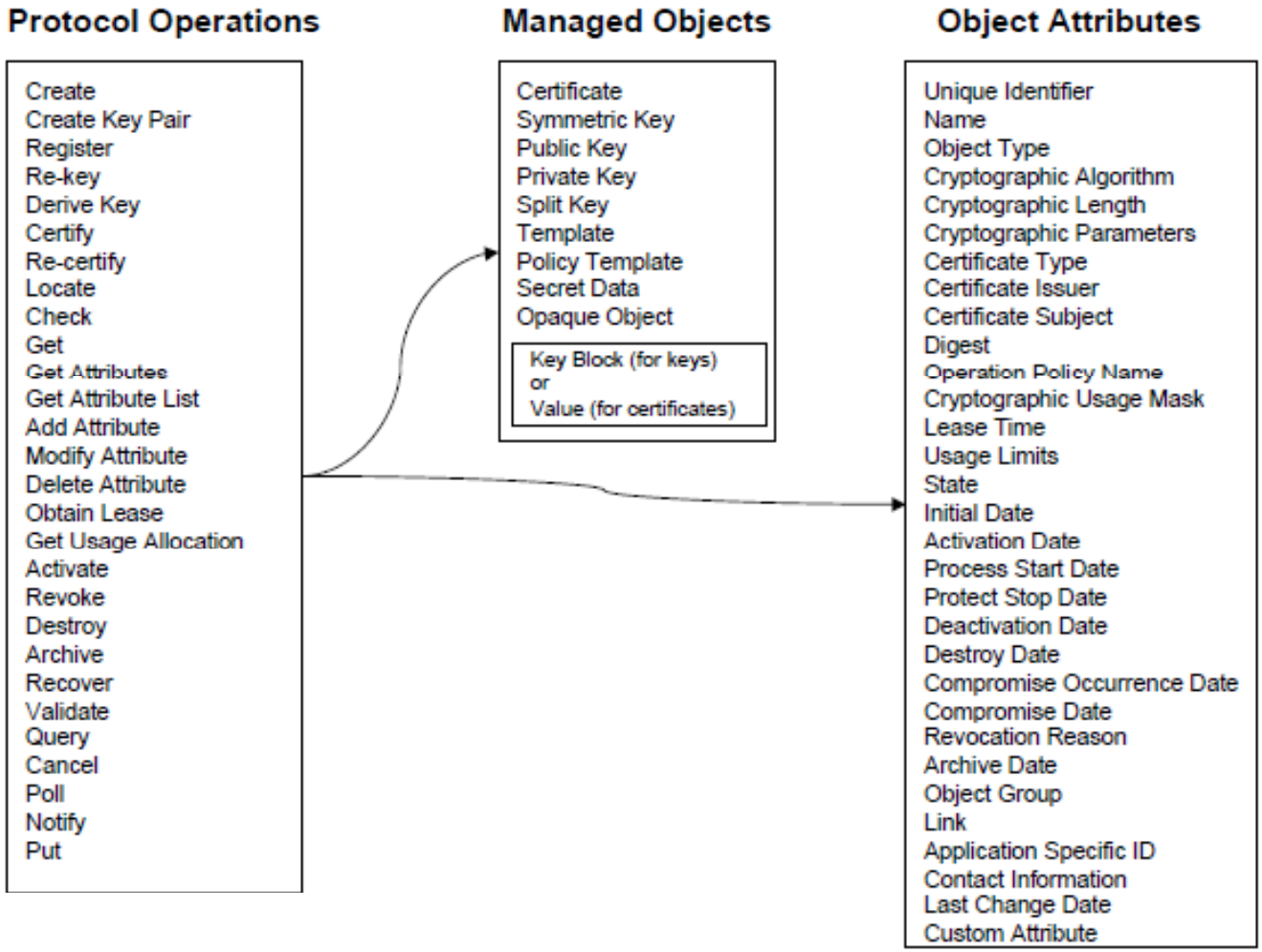
THALES

What is KMIP?

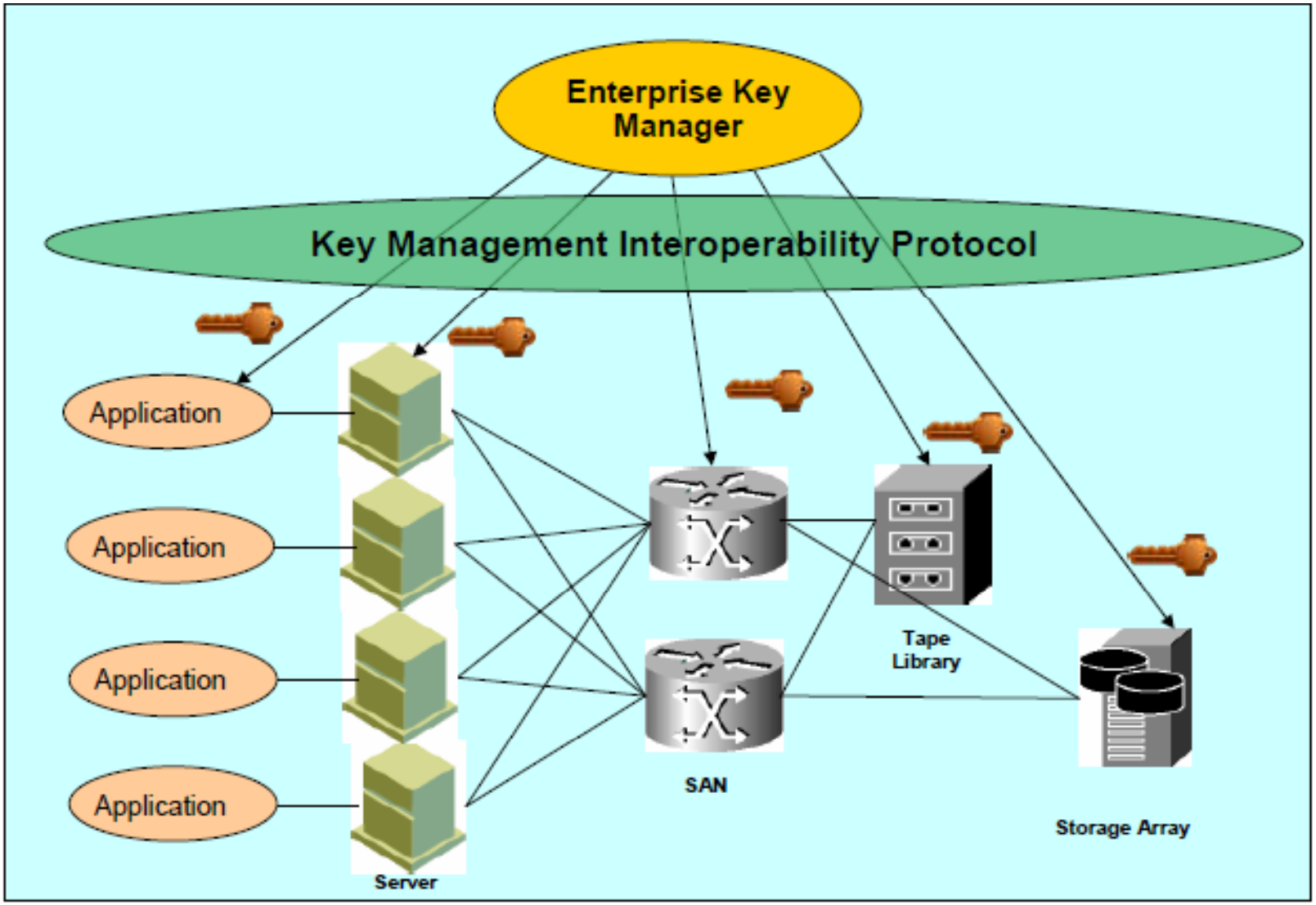
- Key Management Interoperability Protocol (KMIP) は鍵のライフサイクル管理を可能にする
- KMIP は以下をサポートする:
  - 新旧の暗号アプリケーション
  - 対称鍵、非対称鍵
  - デジタル証明書および他のシェアードシークレット
- KMIP は開発者にKMIPアプリケーションの開発と利用を容易にするテンプレートを提供
- KMIP は以下のプロトコルを定義
  - 暗号クライアントと鍵管理サーバー間の通信
  - 鍵のライフサイクル管理 (暗号鍵の生成, 登録, 取得, 削除)
- ベンダーはKMIPに準拠した鍵管理サーバーとの通信をサポートするKMIP暗号アプリケーションを供給する

KMIPはオペレーションのセットを定義する

オペレーションは属性値と暗号要素で構成されるオブジェクトに対して適用

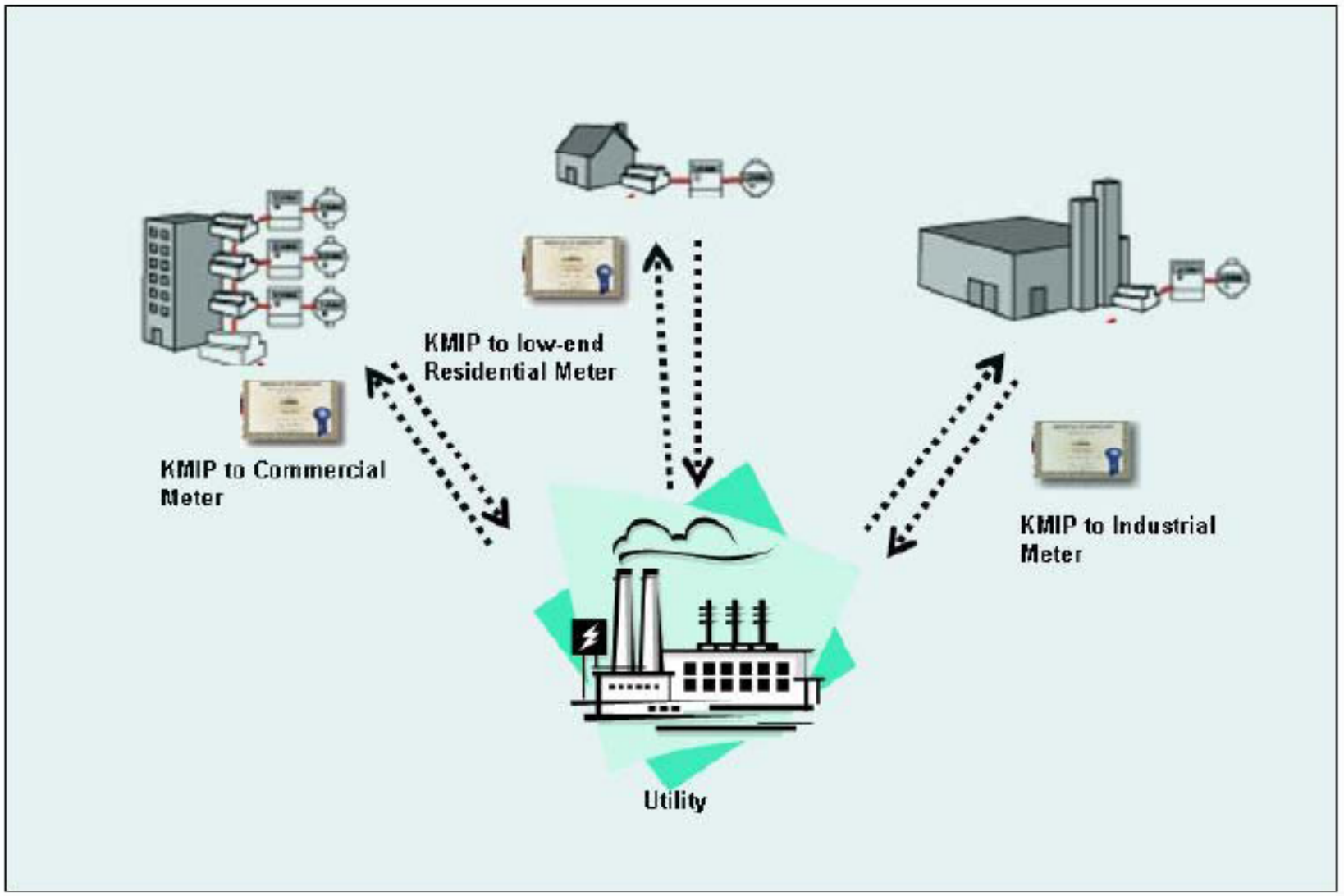


KMIP: Symmetric Encryption Keys



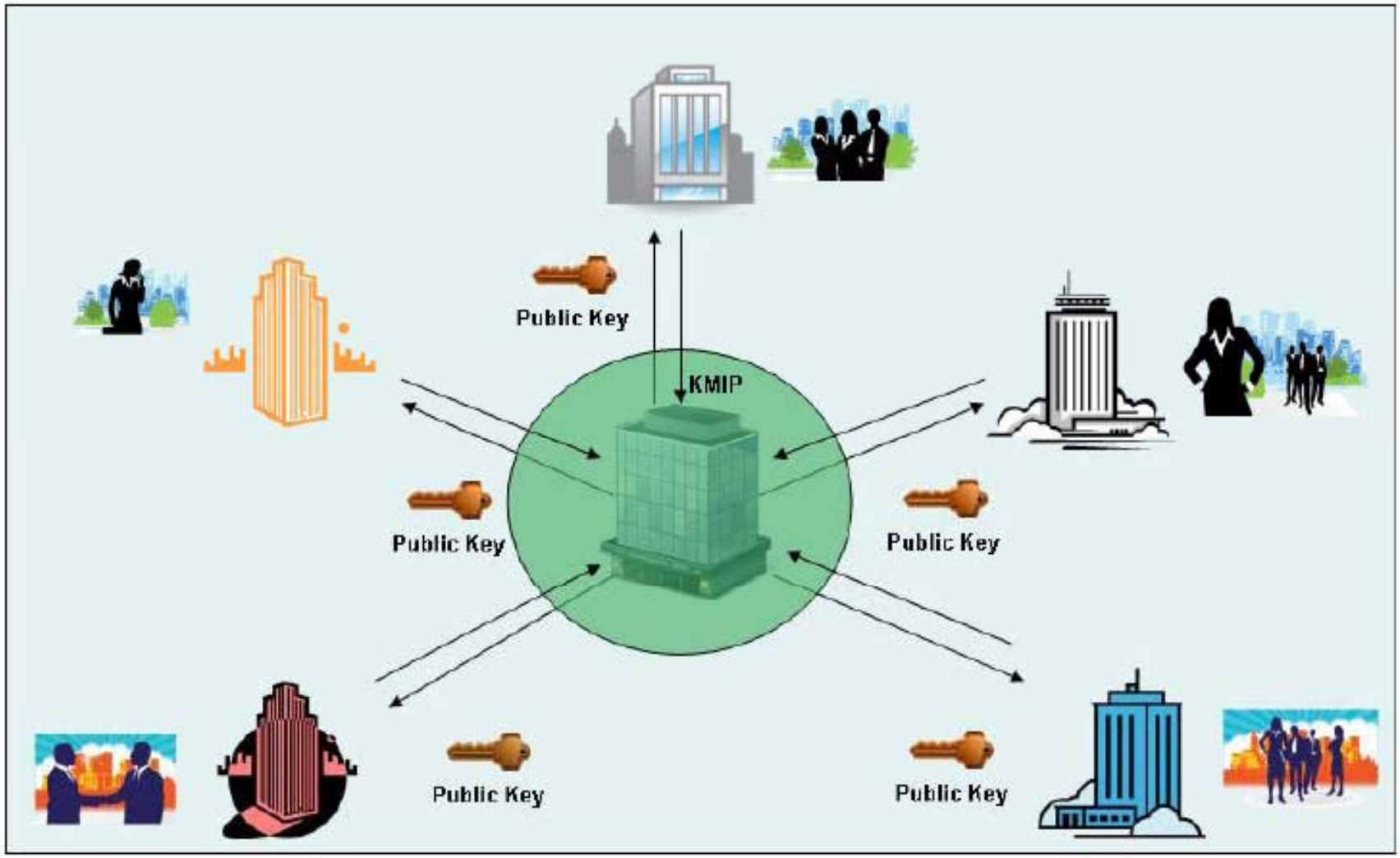
THALES

KMIP: Digital Certificates



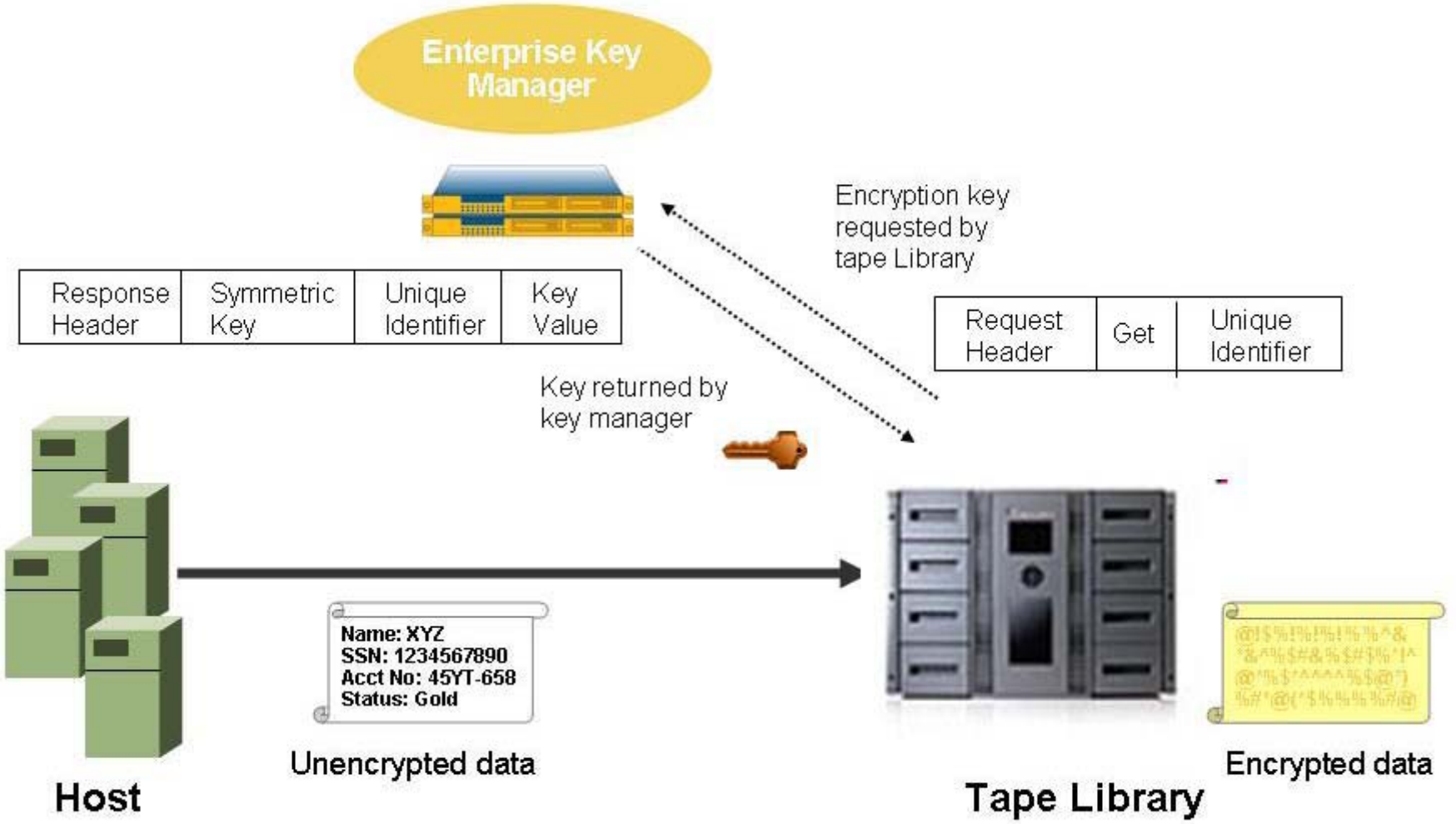
THALES

KMIP: Asymmetric Keys



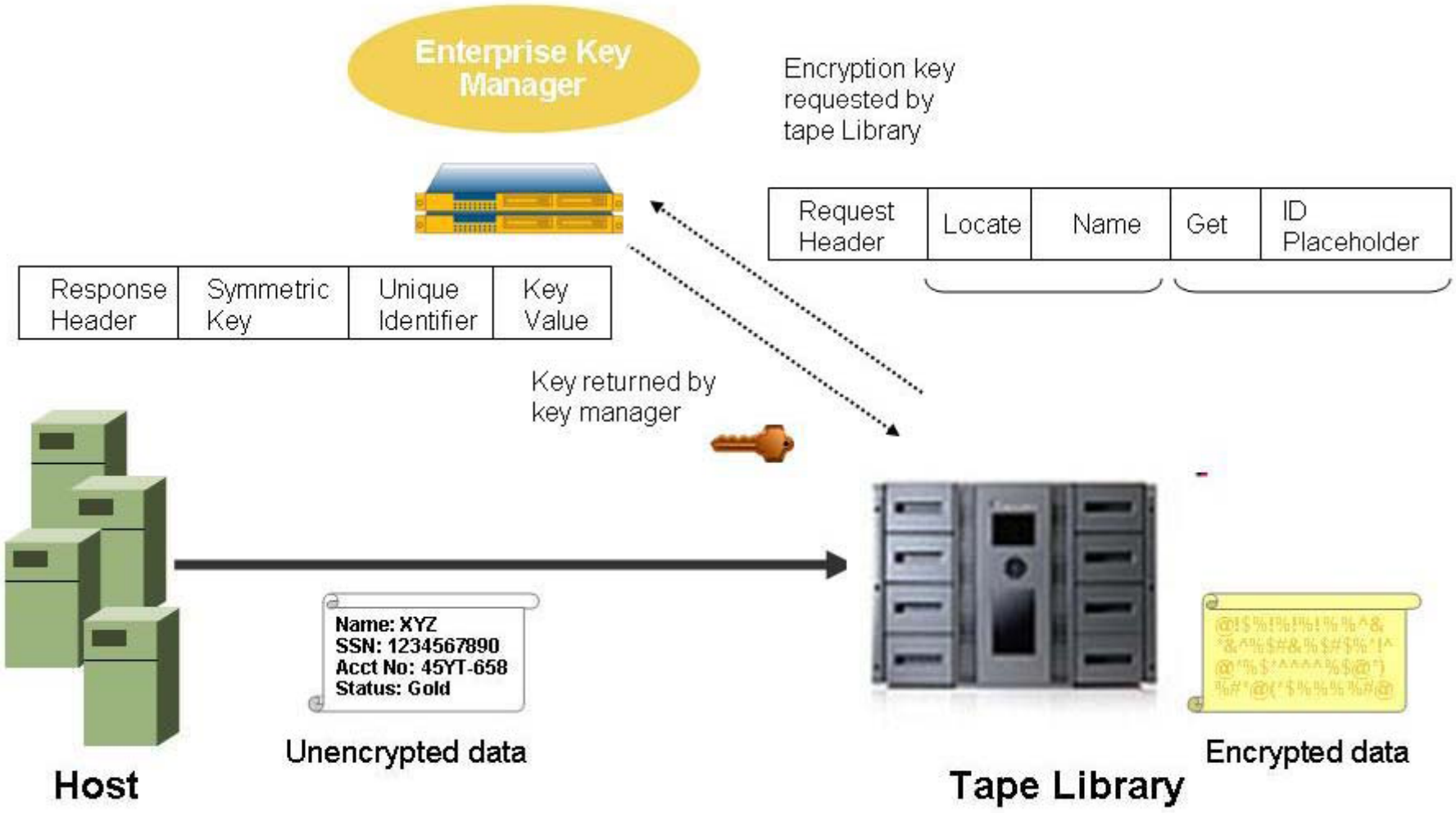
THALES

KMIP Request / Response Model



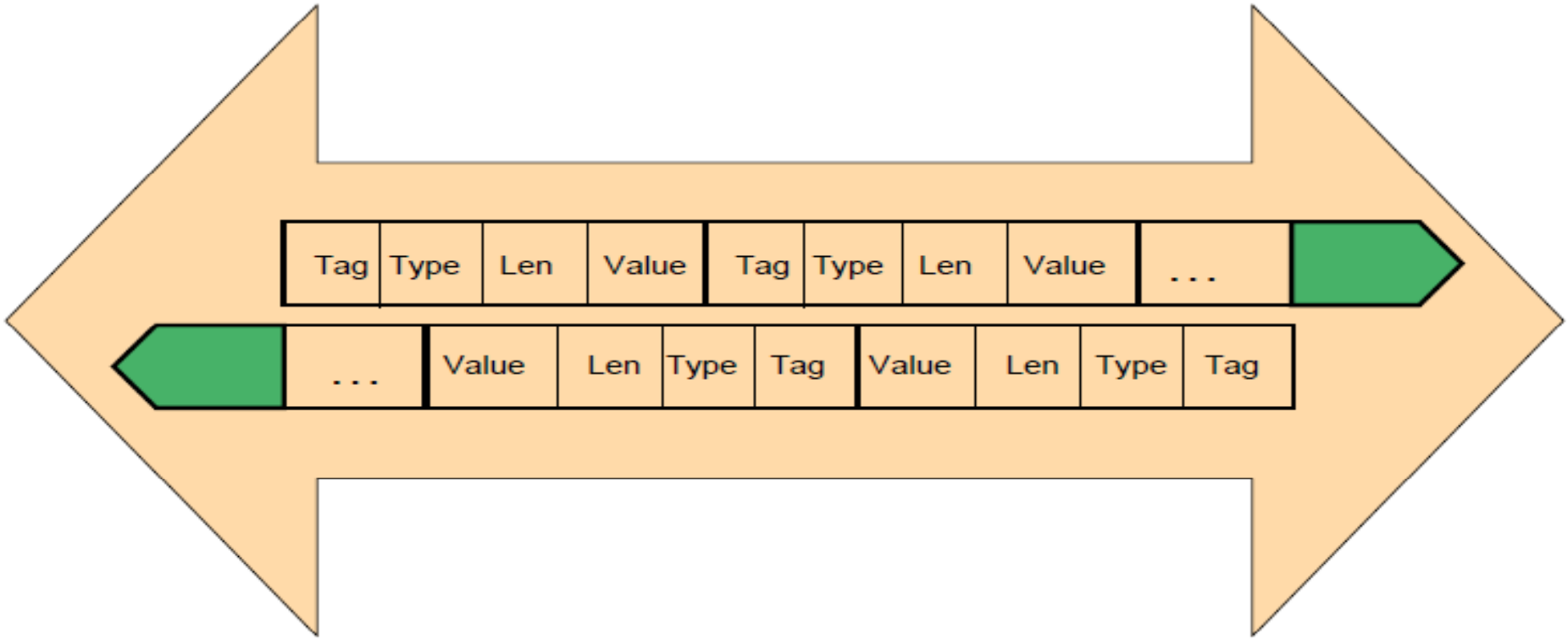
THALES

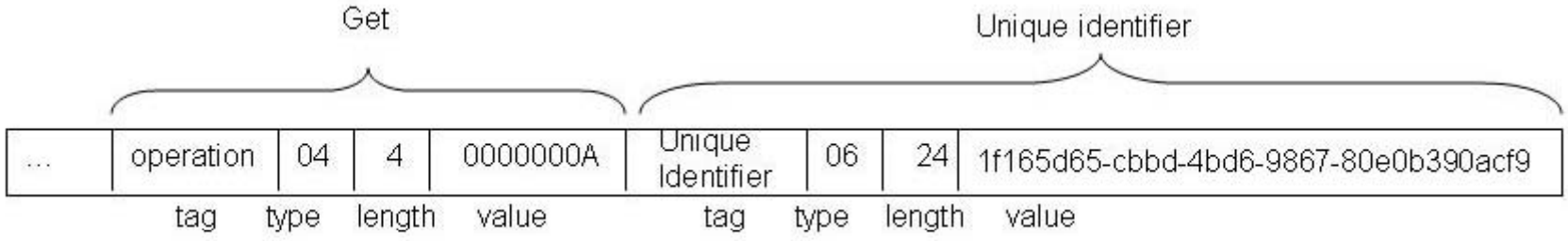
Supporting Multiple Operations per Request



THALES

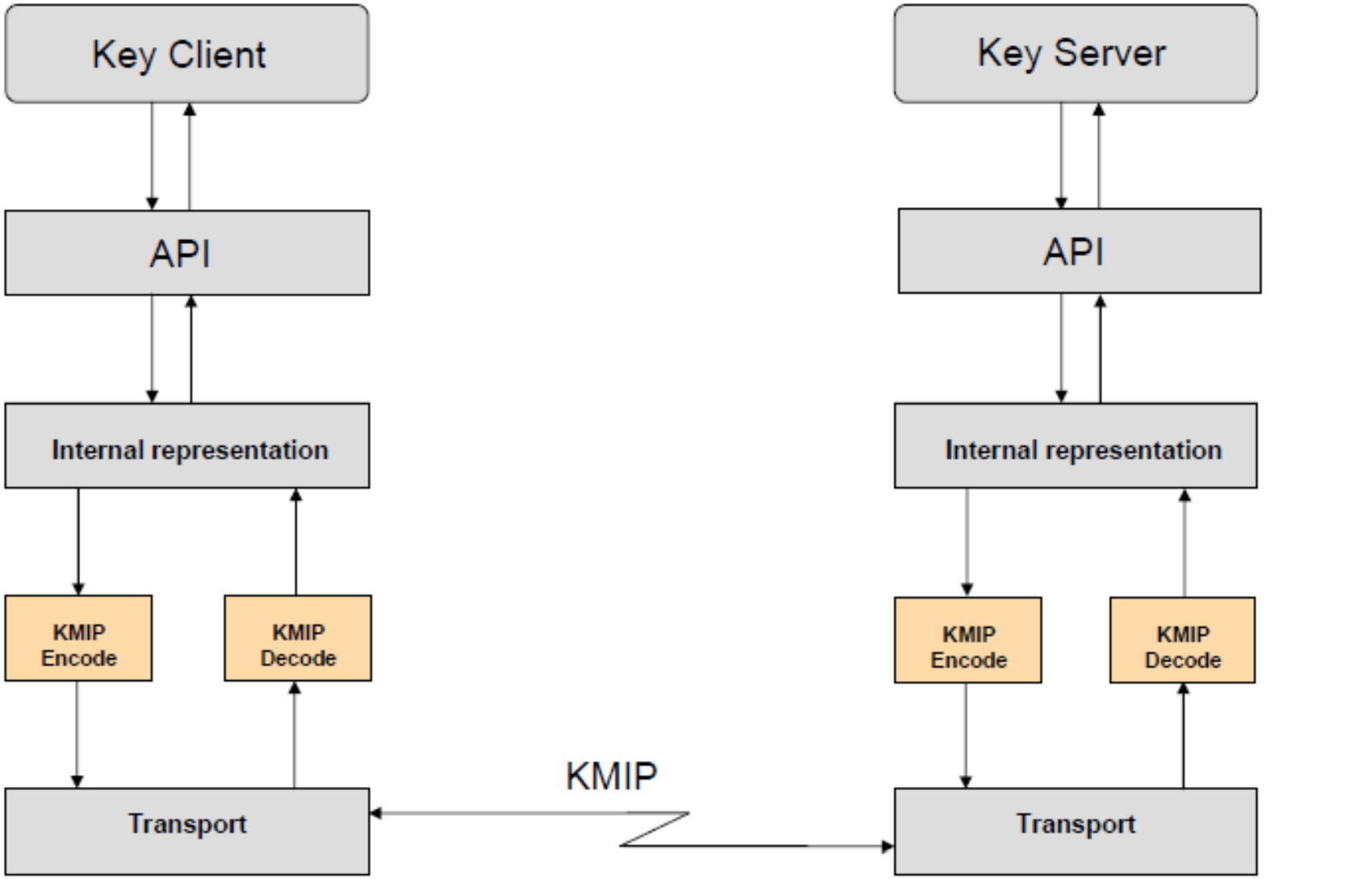
Messages in TTLV Format





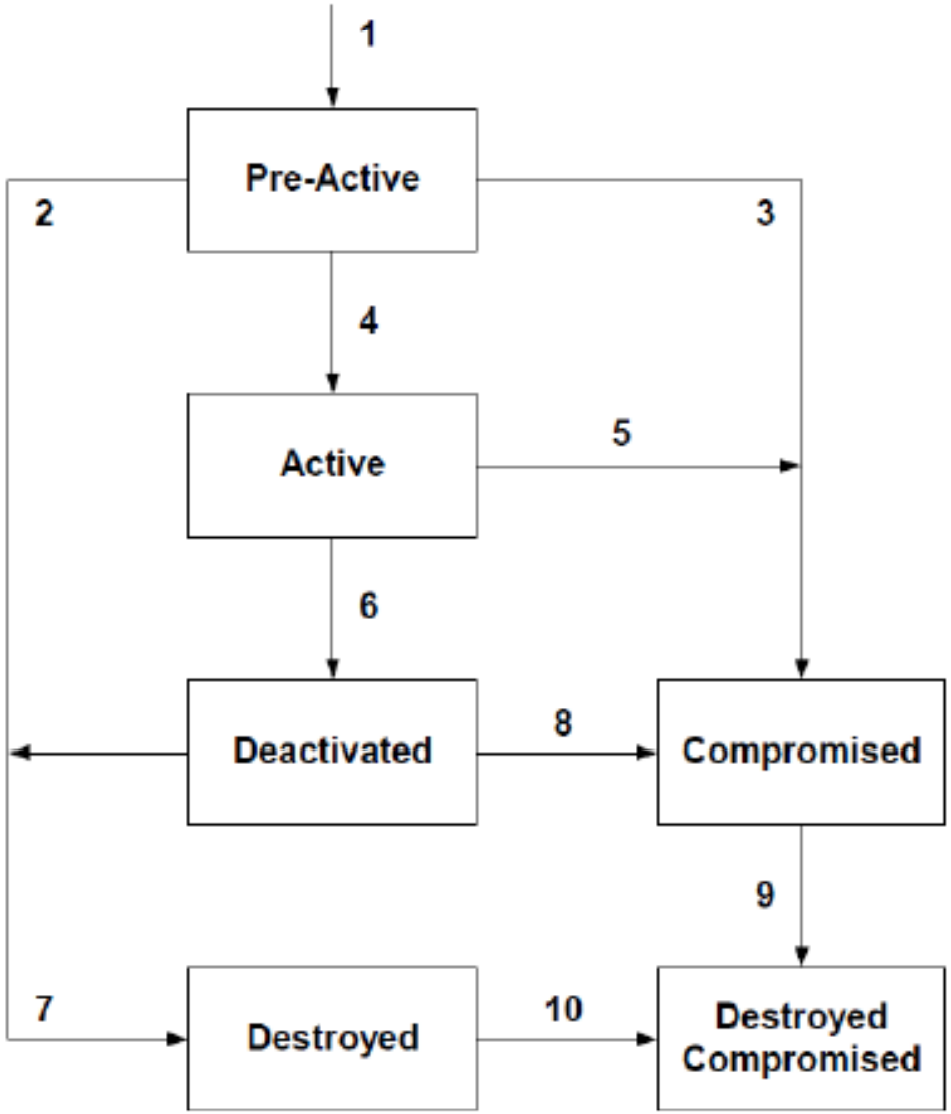
THALES

KMIP Client-Server Request Model



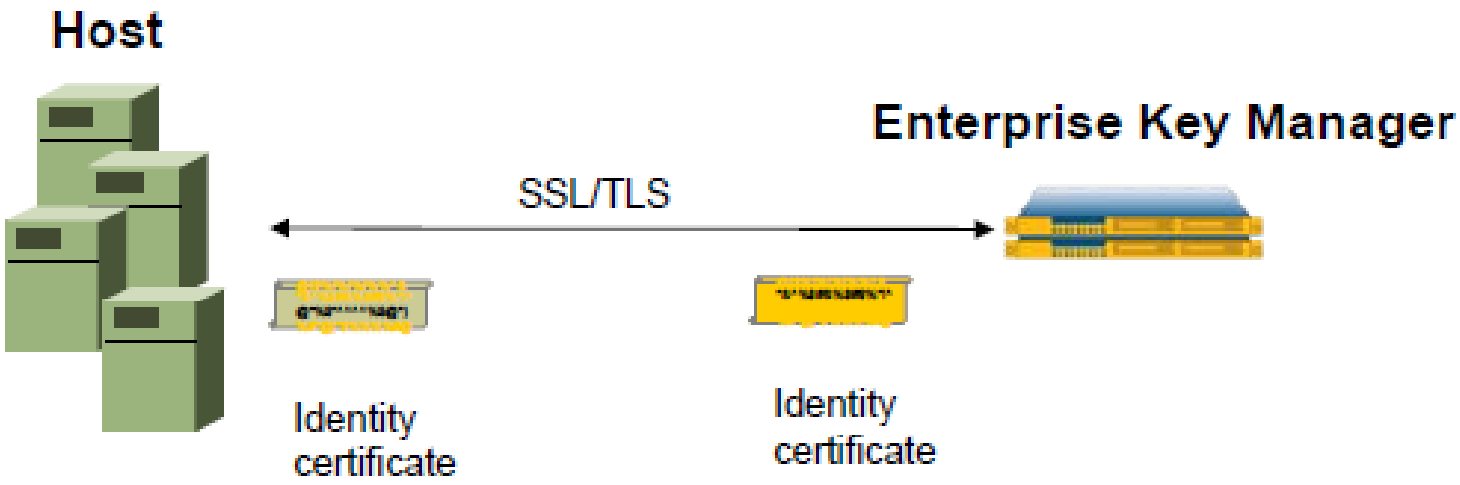
THALES

Key Lifecycle States and Transitions



THALES

- 認証はKMIPプロトコルには含まれない
- 全てのサーバーは少なくとも以下をサポートするべき:
  - SSL/TLS
  - https



- **OASIS** (Organization for the Advancement of Structured Information Standards) はグローバルな情報社会のオープンスタンダードの開発、統合および採用を推進する非営利コンソーシアム
- OASIS KMIP Technical Committee は 2009年3月に発足
  - 発足時メンバー: **Thales**, IBM, HP, RSA.
  - Enterprise Key Management (EKM) サービスとEKMクライアントの相互運用についての仕様を開発
  - この仕様により以下の要求事項に対処する:
    - 鍵のライフサイクル管理 (生成, 配布, 利用, アーカイブ, 破棄など)
    - 鍵の共有、暗号オブジェクトの長期的な可用性 (公開/秘密鍵、証明書、対称鍵など)

How does this work compare with related standards efforts?

- OASIS KMIP TC に関連するいくつかの取り組み:
  - OASIS EKMI TC

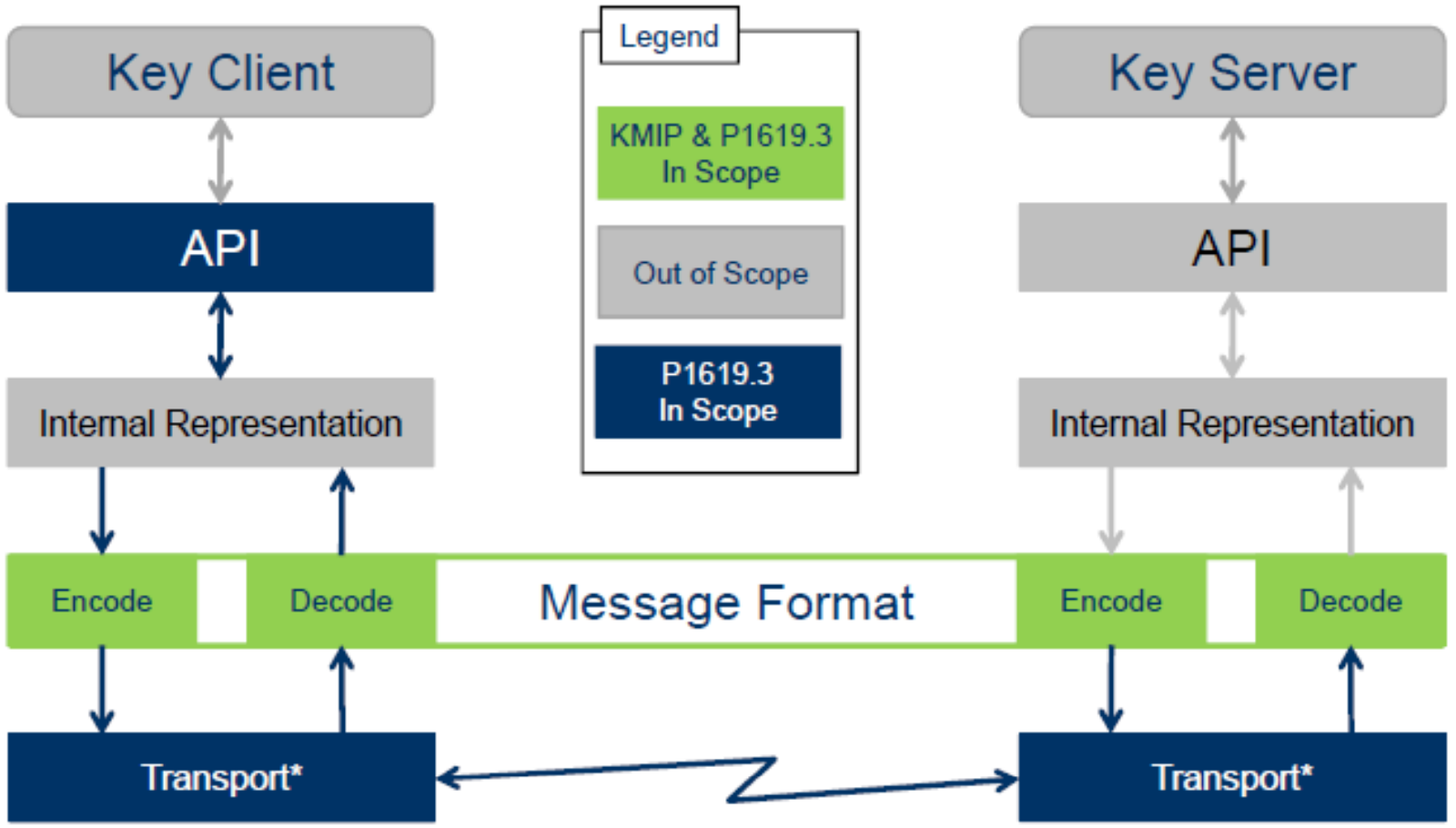
    KMIP TCは主に対称鍵にフォーカスしているEKMIよりも包括的なプロトコルを提供し、より広範囲なスコープで対応
  - IEEE P1619.3

    KMIP TCは主にストレージに関連したP1619.3よりも広範囲なスコープで対応
  - TCG Infrastructure Working Group

    KMIP TCは主にTPMに関連したTCG IWGよりも広範囲なスコープで対応
  - IETF Keyprov

    KMIP TCは主にモバイルに関連したIETF Keyprovよりも広範囲なスコープで対応

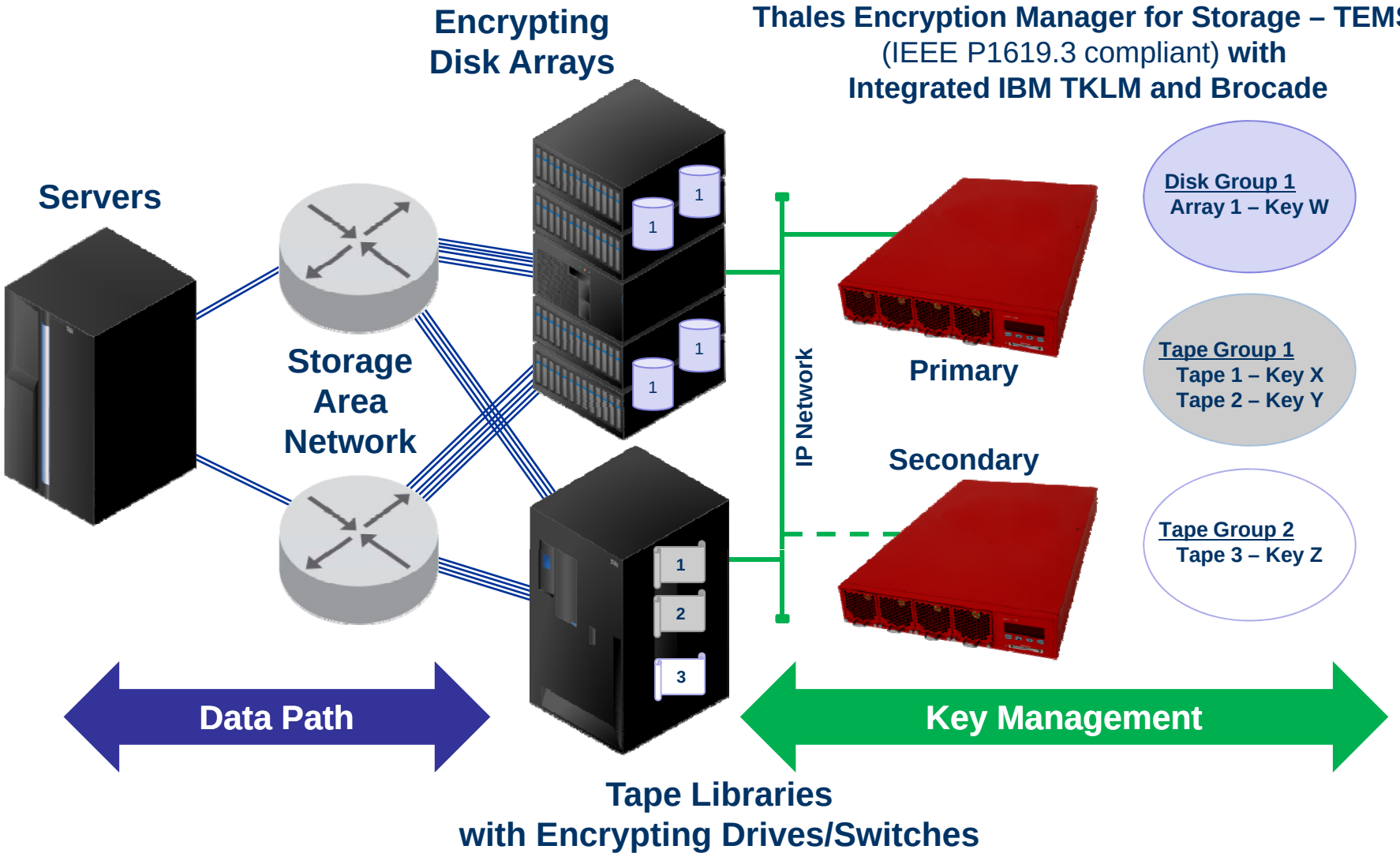
How P1619.3 Relates to KMIP Transport Level Encoding



* Transport requires a secure communication protocol (e.g. HTTPS, TLS, etc…)

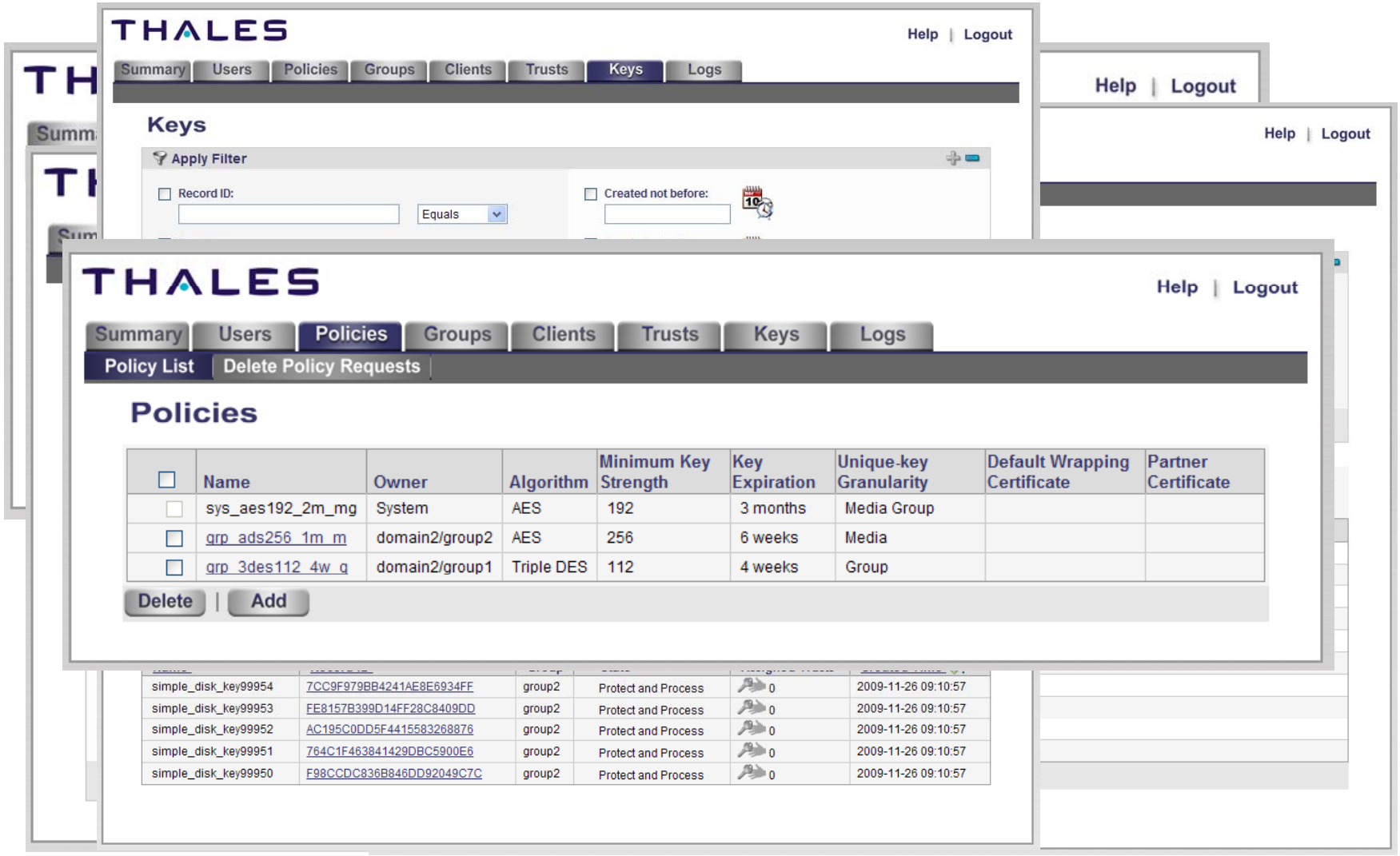
THALES

Example: Centralized Key Management for Storage



THALES

Secure Web Management Interface



THALES

Example: Centralized Key Management for Database

Data encryption keys

DB#1

DB#2

DB#3

data

Database client applications

FIPS VALIDATED 140-2

Common Criteria

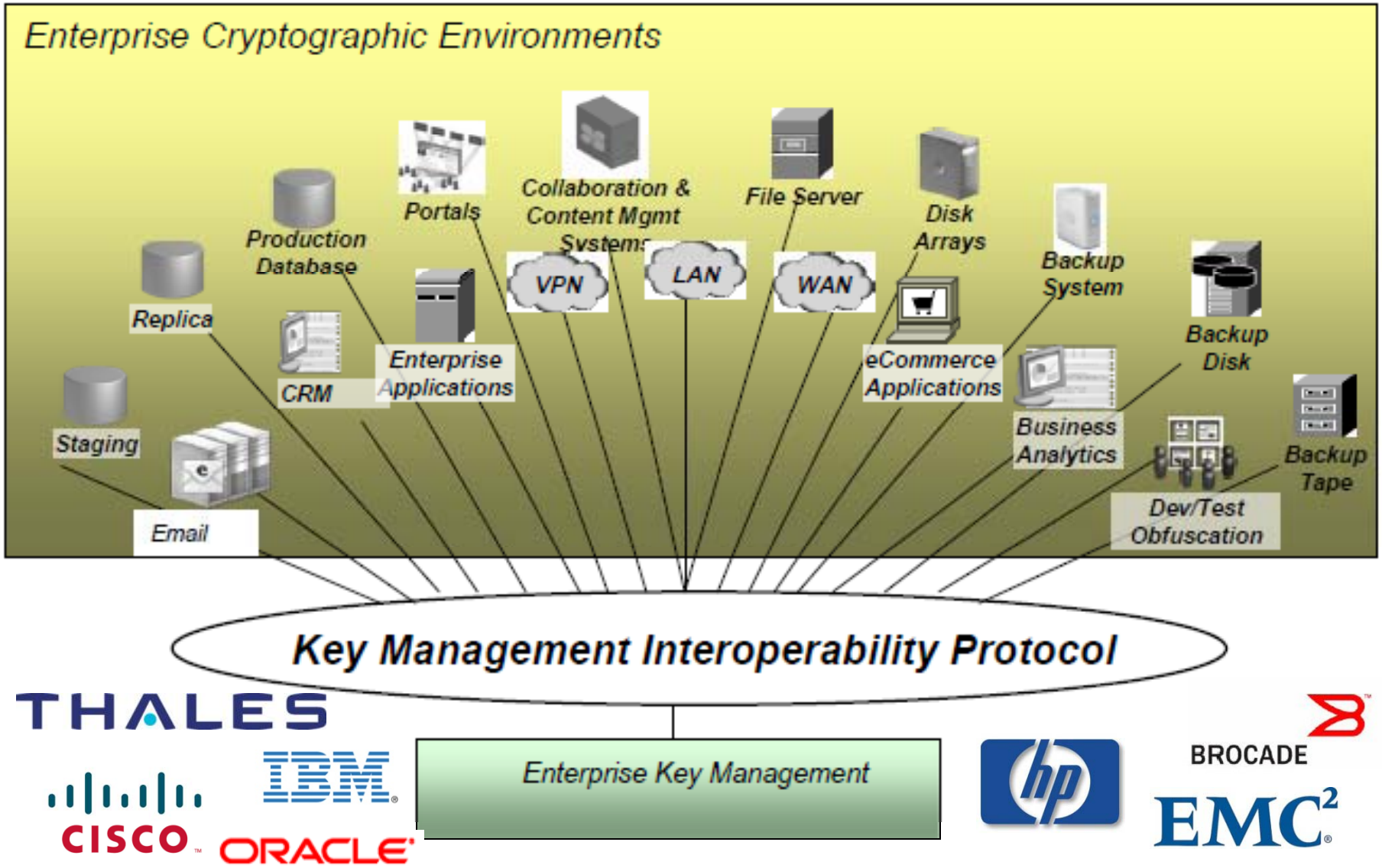
HSMs add value:

- Operational benefits
- Security benefits
- Compliance benefits

Global Trends

- データ漏洩を防ぐ、セキュリティ要件に従いコンプライアンスを実施する、暗号管理の監査を容易にする
- ベンダー依存ではない、市場からの要求に応じた広範なデバイスのサポート
- 導入と展開が容易な堅牢なアプライアンス;ソフトウェアソリューションや手動処理よりセキュア
- 標準ベースのアプローチは相互運用を容易にし、標準ベースの新しい暗号デバイスに対するサポートを提供する
- 異機種環境にまたがった鍵管理は、メンテナンスを容易にし、管理者権限を統合する
- フィールドで実証された拡張性と、緻密な鍵管理ポリシーへの適合性

KMIP: enabling enterprise key management through standard protocol



THALES

- R&DへのThales投資額合計 22億ユーロ (年間売上げの18%)
- 25,000名の最先端技術に関する研究者
- 年間300 の発明特許申請
- 15,000 以上の特許保有
- ヨーロッパ・米国・アジアの30 以上の大学や公共の研究機関と提携

Albert Fert

アルベール・フェール

国立科学研究センター(CNRS)と
THALESの合同研究室科学主任

２００７年

ノーベル物理学賞受賞

巨大磁気抵抗の発見者

お問い合わせ先

製品情報：

- **タレス社ISS事業部Webサイト(日本語)**
- **http://iss.thalesgroup.com/ja-JP**

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　ISS事業部**
- 代表：03-5785-1975
- Jpnsales@thales-esecurity.com

ご清聴ありがとうございました

http://itunes.apple.com/jp/app/moonshield/id387682262?mt=8#

http://www.moonshield.com/