THALES

暗号鍵管理のためのHSM

舟木 康浩
タレスDIS CPLジャパン株式会社
Sales Engineering Manager JAPAN
Yasuhiro.Funaki@thalesgroup.com

自己紹介

舟木 康浩　CISSP

Ottawa

Ottawa freezes its way to coldest capital city in the world

オタワの大寒波は歴史的なものとなりつつあり、世界で最も気温の低い首都に

Temperature slipped below those of capitals in Russia, Kazakhstan and Mongolia

CBC News · Posted: Jan 19, 2019 9:44 AM ET | Last Updated: January 19

nds
、NYSE

(Philippe

により、
ュリティ
&ライ

HALES

タレスグループについて

我々のチーム

80,000
従業員数

世界中で

68
カ国に展開

*売上高**

€190おおよそ**億**

バランスの取れた収益構造

60% 民間　**40%** 防衛

*2017年報告のタレスとジェムアルトの損益計算書の合算に基づく

以上の

Hardware Security Modules
#1
worldwide

Advanced defence systems
#1
in Europe
for defence sensors and mission systems

Air Traffic Management
#1
worldwide

In-flight entertainment
#2
worldwide

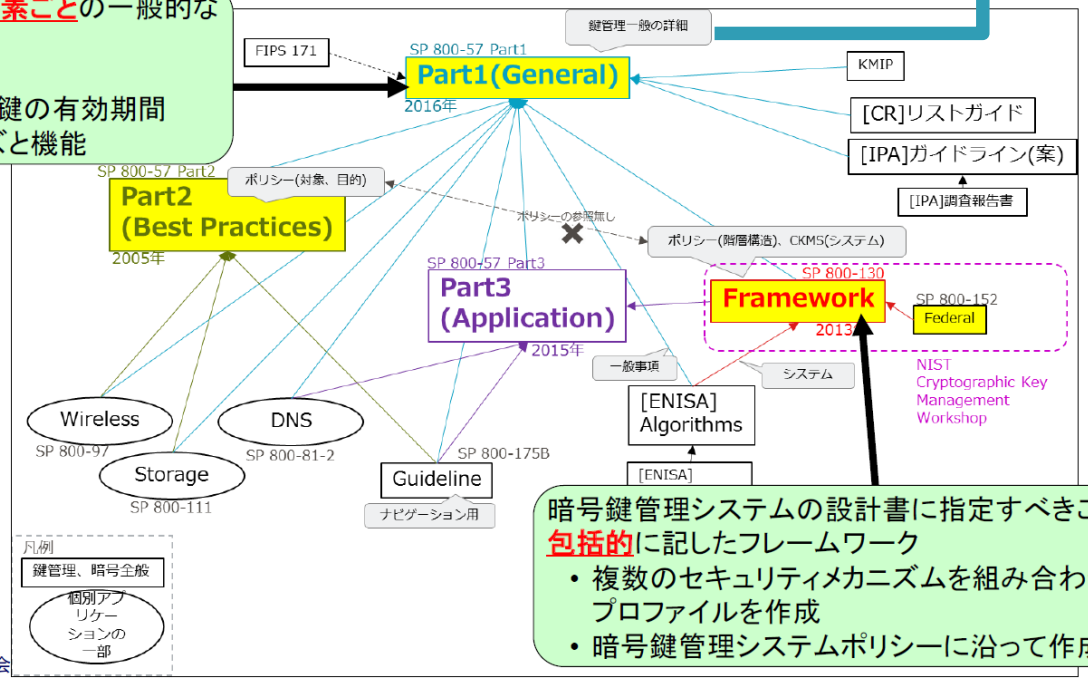
Space solutions
#2
worldwide
(civil satellites)

Rail signalling and supervision
#2
worldwide

Flight avionics
#3
worldwide

ご説明予定の箇所
ハードウェアセキュリティモジュール

鍵管理で扱われる<u>要素ごと</u>の一般的なガイダンス
- 鍵の種別
- 暗号利用期間／鍵の有効期間
- 鍵管理のフェーズと機能



暗号鍵管理システムの設計書に指定すべきことを<u>包括的</u>に記したフレームワーク
- 複数のセキュリティメカニズムを組み合わせてプロファイルを作成
- 暗号鍵管理システムポリシーに沿って作成

NIST SP800-57

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf

5.5.2 Protective Measures

Certain protective measures may be taken in order to minimize the likelihood or consequences of a key compromise. The following procedures are usually involved:

1. Limiting the amount of time that a secret symmetric or asymmetric private key is in plaintext form;
2. Preventing humans from viewing plaintext secret symmetric and asymmetric private keys;
3. Restricting plaintext secret and private keys to physically protected "containers." This includes key generators, key-transport devices, key loaders, cryptographic modules, hardware security modules (HSMs), and key-storage devices;

Cryptographic modules are used to perform cryptographic operations using these keys. This Recommendation does not address the implementation details for cryptographic modules that may be used to achieve the security requirements identified herein. These details are addressed in Federal Information Processing Standard (FIPS) 140 [FIPS 140] and its associated implementation guidance and derived test requirements (available at https://csrc.nist.gov/projects/cmvp/).

https://csrc.nist.gov/publications/detail/fips/140/2/final

FIPS 140-2

Security Requirements for Cryptographic Modules

Date Published: May 25, 2001 (Change Notice 2, 12/3/2002)

Superseded By: FIPS 140-3 (03/22/2019)
Supersedes: FIPS 140-2 (10/10/2001)

Planning Note (3/22/2019): Testing of cryptographic modules against FIPS 140-2 will end on September 22, 2021. See FIPS 140-3 Development for more details.

Author(s)
National Institute of Standards and Technology

https://www.gpki.go.jp/documents/kihon.pdf

(7) 鍵管理機能

公開鍵・秘密鍵ペアの生成、鍵の廃棄、署名、鍵のバックアップを行う。秘密鍵は、NIST（National Institute of Standards and Technology：米国標準技術研究所）の FIPS（Federal Information Processing Standards）140-1 レベル３又は FIPS140-2 レベル３相当以上の耐タンパ鍵装置 HSM（Hardware Security Module）で生成・管理する。

THALES

HSMはさまざまなガイドライン等で言及

IoT開発におけるセキュリティ設計の手引き

https://www.ipa.go.jp/files/000052459.pdf

- 「暗号」に対する多数の言及
- 各種ガイドライン等でも暗号技術は必須の要素と認識されている
- 鍵管理についても言及され始めている

「HSM」についても以下の通り言及

IoT における暗号技術チェックリスト(2/5)

	暗号技術の詳細項目とセキュリティ要件 （◎必須、○推奨）	参照[38][39][40][41][42][43][44]	チェックリスト回答欄	
			判定	根拠(任意記入欄)
鍵の生成				
9	【共通鍵暗号(共通鍵)を使用している場合】 ◎安全な方法を用いて、鍵を生成すること。 ○共通鍵は、以下のいずれかの方法で生成することが望ましい。 (1) ローカル(鍵を使用する機器内)で、以下のいずれかの方法で生成する。 ・機器配布前に疑似乱数生成アルゴリズムに初期 seed を設定し、稼働中の不確定要素を用いて seed を更新して鍵生成する。	・NISTIR 7628: 4.2.1.2, 4.2.2.3		

「･･･不正アクセスへの対策を行う。特に暗号鍵、証明書等の枢要なデータについては、鍵管理機能等を有するソフトウェアによる保護又は必要に応じて専用の暗号装置(HSM等)の利用等を検討する。」

11	【共通鍵暗号(共通鍵)を使用している場合】 ◎共通鍵は、完全性および機密性を満たす条件の下で配布すること。 ○鍵の配布に用いるメカニズム(例:暗号アルゴリズム)は、少なくとも鍵と同等の強度を持っていることが望ましい。	・FIPS SP800-57 Part 1: 6.1.1 ・NISTIR 7628: 4.2.2.3, 4.3.3.3		
12	【公開鍵暗号(公開鍵／秘密鍵のペア)を使用している場合】 ◎公開鍵は完全性を、秘密鍵は完全性および機密性を満たす条件の下で配布すること。 ○鍵の配布に用いるメカニズム(例:暗号アルゴリズム)は、少なくとも鍵と同等の強度を持っていることが望ましい。	・FIPS SP800-57 Part 1: 6.1.1 ・NISTIR 7628: 4.3.3.3		
鍵の保管				
13	【共通鍵暗号(共通鍵)を使用している場合】 ◎共通鍵は、完全性および機密性を満たす条件の下で保管すること。 ○永続的に利用する共通鍵は、耐タンパー性を有する H/W(例:暗号専用回路を持つ IC)の内部で保管することが望ましい。	・FIPS SP800-57 Part 1: 6.1.1 ・NISTIR 7628: 4.2.2.3, 4.3.3.3		
14	【公開鍵暗号(公開鍵／秘密鍵のペア)を使用している場合】 ◎公開鍵は完全性を、秘密鍵は完全性および機密性を満たす条件の下で保管すること。 ○秘密鍵は、耐タンパー性を有する H/W(例:HSM、暗号専用回路を持つ IC)の内部で保管することが望ましい。	・FIPS SP800-57 Part 1: 6.1.1 ・NISTIR 7628: 4.1.2.4.2, 4.3.3.3		
鍵の用途				
15	○一つの鍵は、単一の用途(例:暗号化、認証、鍵ラッピング、乱数生成、電子署名)で利用することが望ましい。 ・単一の暗号鍵の暗号処理が同時に複数の機能を実現する場合(例:署名と認証、暗号化と認証)を除く。 ・鍵共有／鍵配送用途の公開鍵／秘密鍵ペアに対する公開鍵証明書発行要求のための電子署名を除く。	・FIPS SP800-57 Part1: 5.2		

ハードウェアセキュリティモジュール宣言（皆様への価値）

免責事項：個人の見解です

Amazon Web Service

https://pages.awscloud.com/rs/112-TZM-766/images/AWS-28_AWS_Summit_Online_2020_MAD01.pdf

開発者の作業を阻害しないITインフラをAPI経由で可能にするコンピュートリソース

ハードウェアセキュリティモジュール

ITインフラの鍵管理に対して説明責任を可能にするコンピュートリソース

経営者(サービス事業者）に

監査者に

設計者に

運用者に

鍵利用者に

HSM(ハードウェアセキュリティモジュール)

1. 鍵のオーナーシップ
2. 信頼の頂点–秘密鍵を外部に出さない運用が可能
3. 鍵の管理＋暗号処理もHSM内部で実行
4. 専用チップによる高速/セキュリティ処理
5. 第3者にセキュリティ機能の説明が容易

THALES

HSM進化の過程

https://cpl.thalesgroup.com/encryption/hardware-security-modules/network-hsms

専用HSM

単一のアプリケーション

ネットワーク型HSM

複数のアプリケーション

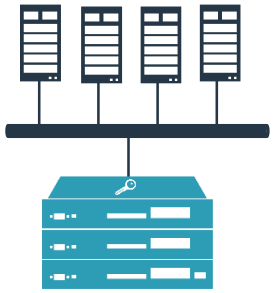
複数パーティション

複数のお客様/アプリケーション

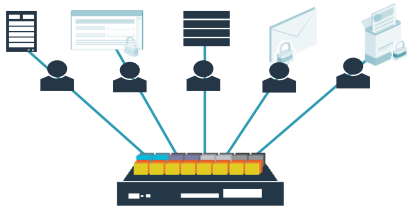
クラウドHSMサービス

サブスクリプション/サービスモデル

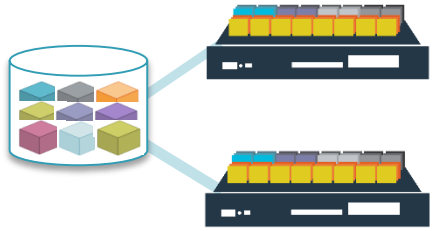
1995
Luna CA3



2002
Luna SA/IS



2013
Luna Network HSM



2017
DPOD Luna Cloud HSM

暗号アルゴリズムはファームウェアで提供することでCrypto Agility(迅速性)を提供

THALES

経営者層へのメッセージ

“企業は自身で鍵管理を運用することが求められます”

IDCの発表 – 国内情報保護／ガバナンス製品市場予測 (2019年11月19日)

- https://www.idc.com/getdoc.jsp?containerId=prJPJ45640619
- 国内暗号化／鍵管理市場の2018年～2023年の年間平均成長率（CAGR：Compound Annual Growth Rate）は3.3%で、市場規模（売上額ベース）は2018年の136億円から、2023年には160億円に拡大すると予測
- 暗号化／鍵管理市場は、大規模な情報漏洩事件によってデータ侵害への危機意識が高まり、データ侵害に対するガバナンス強化への対策需要として市場が拡大
- 今後は、デジタルトランスフォーメーション（DX）が進展することで、クラウド上での構造化データおよび非構造化データの活用が拡大し、**構造化データと非構造化データの両者のデータに対する暗号化と鍵管理、情報漏洩対策が必要**
- 機密性の高いワークロードをクラウドに移行する際には、**企業は自身で鍵管理を運用することが求められる**
- このような企業では、**クラウドネイティブな暗号化と鍵管理**、そしてクラウド型DLPソリューションへの需要が拡大する

鍵管理に関する監査対応/説明責任

鍵管理セキュリティの基準/FIPS140-2(3)

各取得した製品のセキュリティポリシーは公開

- https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search

3231	Gemalto	ProtectServer Internal Express 2 (PSI-E2)	Hardware	07/12/2018 01/31/2019
3211	Gemalto	Hardware Security Module	Hardware	06/27/2018
3210	Gemalto	SafeNet USB Hardware Security Module	Hardware	06/27/2018
3209	Gemalt		Hardware	06/27/2018
3208	Gemalt	Net PCIe Hardware Security	Hardware	06/26/2018
3198	Gemalt		Hardware	06/14/2018
3182	Gemalt		Hardware	05/02/2018 05/17/2018 06/13/2019

証書番号を選択することで製品のセキュリティポリシーを参照可能

Certificate #3182

Details

Module Name	SafeNet Luna K7+ Cryptographic Module
Standard	FIPS 140-2
Status	Active
Sunset Date	5/1/2023
Validation Dates	05/02/2018;05/17/2018;06/13/2019
Overall Level	3
Caveat	When operated in FIPS mode and initialized to Overall Level 3 per Security Policy
Security Level Exceptions	• Physical Security: Level 4
Module Type	Hardware
Embodiment	Multi-Chip Embedded
Description	The SafeNet Luna K7+ Cryptographic Module is a high-assurance Hardware Security Module with a tamper-active physical enclosure, which secures sensitive data and critical applications by storing, protecting and managing cryptographic keys. It provides end users with industry-leading security and performance, and can quickly be embedded directly into servers and security appliances for FIPS 140-2 validated key security. The module meets compliance and audit needs for FIPS 140, HIPAA, PCI-DSS, eIDAS, GDPR, and is suitable for deployment in less controlled physical environments.

FIPS Algorithms	
AES	Certs. #4753 and #4754
CVL	Cert. #1392 and #1431
DRBG	Cert. #1634
DSA	Cert. #1274 and #1275
ECDSA	Cert. #1188 and #1189
HMAC	Cert. #3166
KAS	Certs. #133 and #134
KBKDF	Cert. #152
KTS	AES Cert. #4753; key establishment methodology provides between 128 and 256 bits of encryption strength
RSA	Cert. #2597, #2598, and #2632
SHS	Cert. #3896, #3897, and #3952
Triple-DES	Cert. #2525
Triple-DES MAC	Triple-DES Cert #2525, vendor affirmed

Allowed Algorithms	AES (Cert. #4753, key unwrapping; key establishment methodology provides between 128 and 256 bits of encryption strength); Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength); NDRNG; RSA (key wrapping; key establishment methodology provides between 112 and 152 bits of encryption strength); Triple-DES (Cert. #2525, key unwrapping; key establishment methodology provides 112 bits of encryption strength)
Hardware Versions	808-000069-001, 808-000070-001
Firmware Versions	7.0.1, 7.0.2, 7.0.3, 7.3.3

Vendor

Gemalto
20 Colonnade Road, Suite 200

Related Files

Security Policy
Consolidated Certificate

鍵管理システムの監査/設計/運用時に説明が楽になる機能が記載されています、一緒にFIPSドキュメントを参照してみましょう

THALES

開発者はアプリケーションに集中
各種APIご用意

タレス提供　お客様準備

サーバ(Win/Lin/Unix)

Thales Luna Network HSMの例

アプリケーション

OPENSSL

HSMクライアント

PKCS#11ライブラリ(C/JAVA)
マイクロソフトAPI
JCA/JCE
OPENSSLエンジン
お客様独自API

コンフィグファイル

TCP/IP(NTLS)

TLS

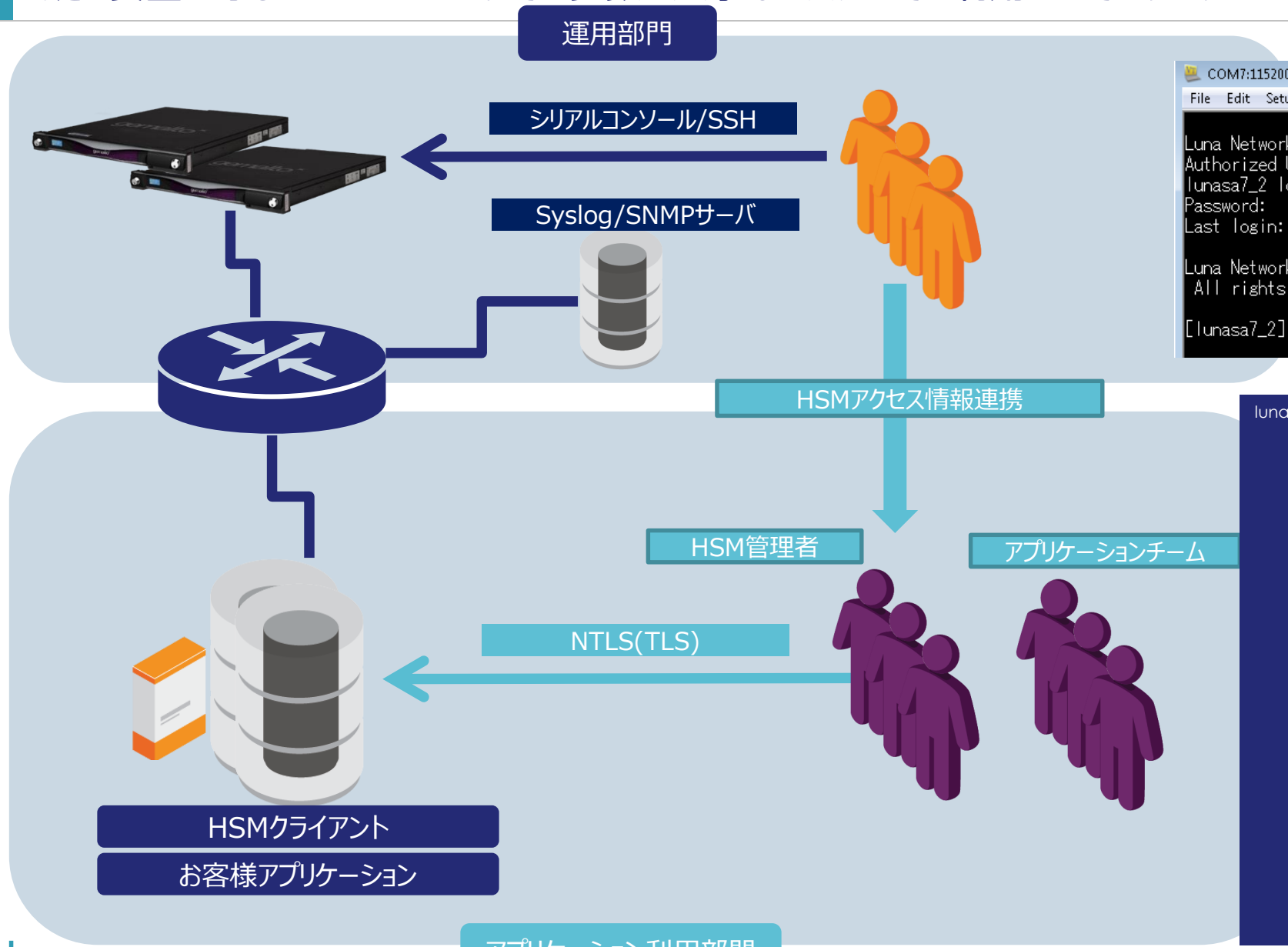
PIN入力専用デバイス

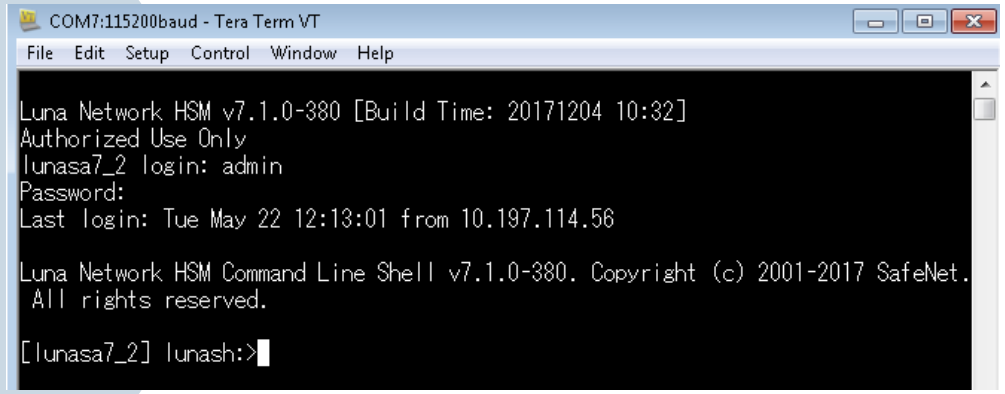
https://www.ipa.go.jp/security/fy15/reports/sec_api/documents/api2003_4.pdf

THALES

HSMシステム設計/運用

鍵を安全に守るためにHSMはすでに多数の大事なシステムでご利用されております



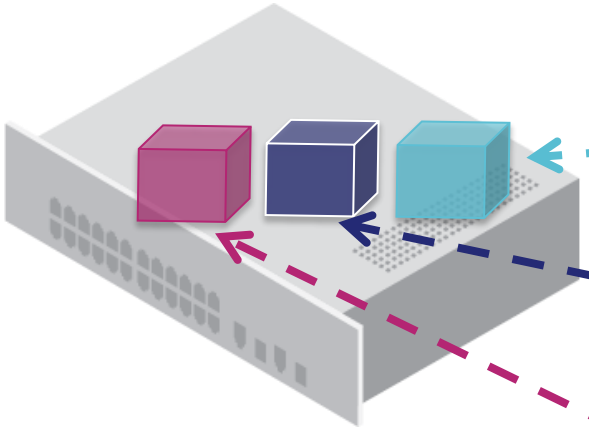



```
lunacm:>par si

        Partition Label ->
        Partition Manufacturer -> Safenet, Inc.
        Partition Model -> Luna NetWork HSM 7.0.0
        Partition Serial Number -> 1283350625688
        Partition Status -> L3 Device, Zeroized
        HSM Part Number -> 808-000066-001
        Token Flags ->
                CKF_LOGIN_REQUIRED
                CKF_RESTORE_KEY_NOT_NEEDED
        RPV Initialized -> Not Supported
        Slot Id -> 0
        Session State -> CKS_RW_PUBLIC_SESSION
        Role Status ->   none logged in
        Token Flags ->
        Partition OUID: 0c0000010000000011b690800

        Partition Storage:
                Total Storage Space:  3345795
                Used Storage Space:   0
                Free Storage Space:   3345795
                Object Count:         0
                Overhead:             9648

        *** The partition is NOT in FIPS 140-2 approved operation mode. ***
```

鍵の所有権

パーティション機能により1台で複数アプリケーション対応

1台のHSMに仮想的に複数のHSMがあるかのようにアプリケーションは利用可能



PIN

PIN

PIN

アプリA：パーティションAを利用

アプリB:パーティションBを利用

アプリC：パーティションCを利用

各パーティション毎に管理者/ポリシーを設定可能
例、パーティションAは秘密鍵取り出し不可/PINリセット可能

鍵の所有権

鍵ごとにユーザ認証(今年リリース予定)

HSM内部で管理される各オブジェクトはPKCS#11に準拠して属性を持つことが可能です

Key
- Key Type
- ID
- Start date
- End date
- Derive
- Local

Local属性でHSM外部で作成されたか判別可能

Public Key
- Subject
- Subject str
- Encrypt
- Verify
- Verify recover
- Wrap
- Export

Private Key
- Subject
- Subject str
- Decrypt
- Sensitive
- Sign
- Sign recover
- Unwrap
- Extractable
- Always sensitive
- Never extractable
- Usage count
- Exportable
- Import

新属性：パスワード

Secret Key
- Sensitive
- Encrypt
- Decrypt
- Sign
- Verify
- Wrap
- Unwrap
- Extractable
- Always sensitive
- Never extractable
- Exportable
- Export
- Import
- Check value

新属性：パスワード

各鍵の用途を限定可能

HSM外部に暗号化してエクスポート(WRAP)可否

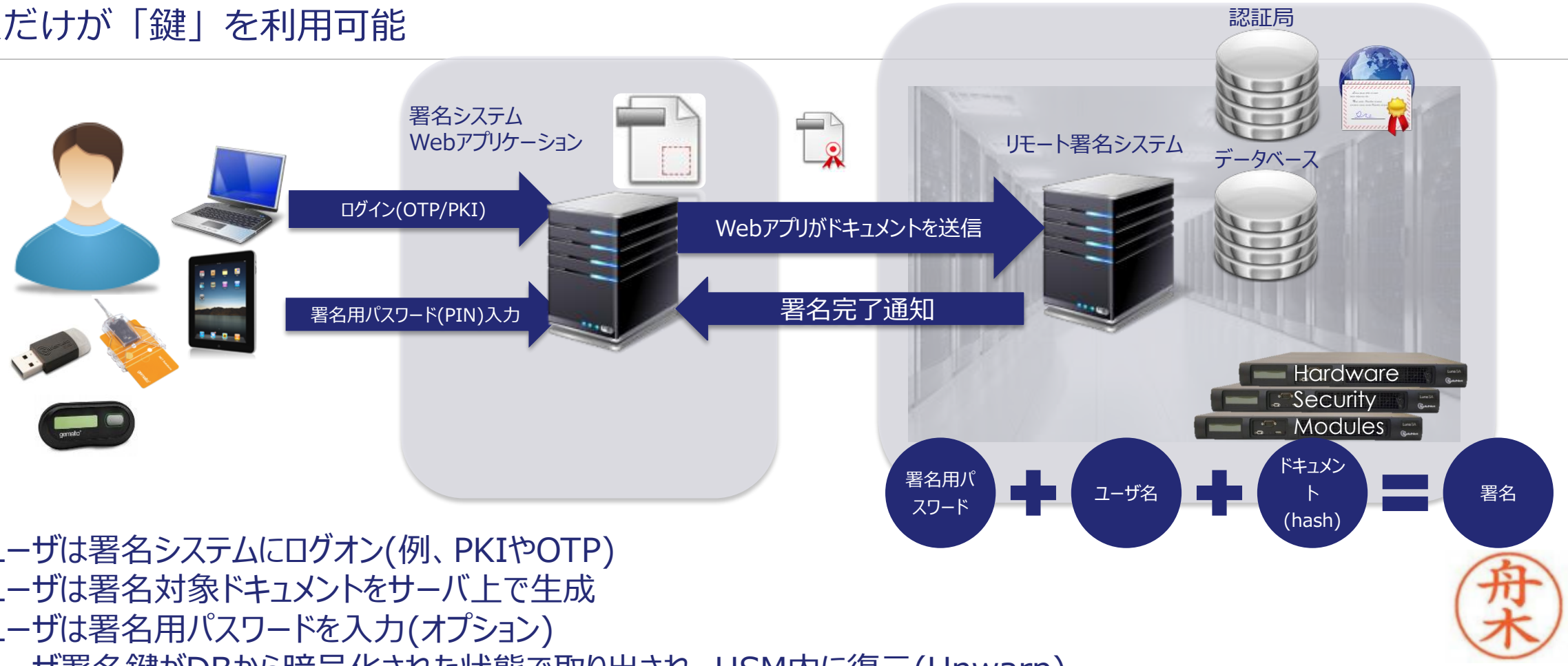
CA_AuthorizeKey

```
CA_AuthorizeKey(
            CK_SESSION_HANDLE hSession,       // the session's handle
            CK_OBJECT_HANDLE  hObject,        // the object's handle
            CK_UTF8CHAR_PTR   pAuthData,      // the user's auth data
            CK_ULONG          ulAuthDataLen   // the length of the auth data
```


THALES

鍵の所有権

本人だけが「鍵」を利用可能



1. ユーザは署名システムにログオン(例、PKIやOTP)
2. ユーザは署名対象ドキュメントをサーバ上で生成
3. ユーザは署名用パスワードを入力(オプション)
4. ユーザ署名鍵がDBから暗号化された状態で取り出され、HSM内に復元(Unwarp)
5. 2で生成されたドキュメントはHSM内の鍵で電子署名
6. 署名されたドキュメントは保存される(アプリケーション要件による)
7. 署名完了をユーザに通知

HSM活用例
大手製造業様

私が入社時の海外事例です

お客様プロファイル

- 世界最大規模の通信装置製造業者

課題

- 自社製品のセキュリティ強化のために、自社製品に対して電子証明書発行とコード署名を実施
- 各部門/工場に自社要件に応じてスケール可能なセキュリティポリシーを中央管理なシステム構築

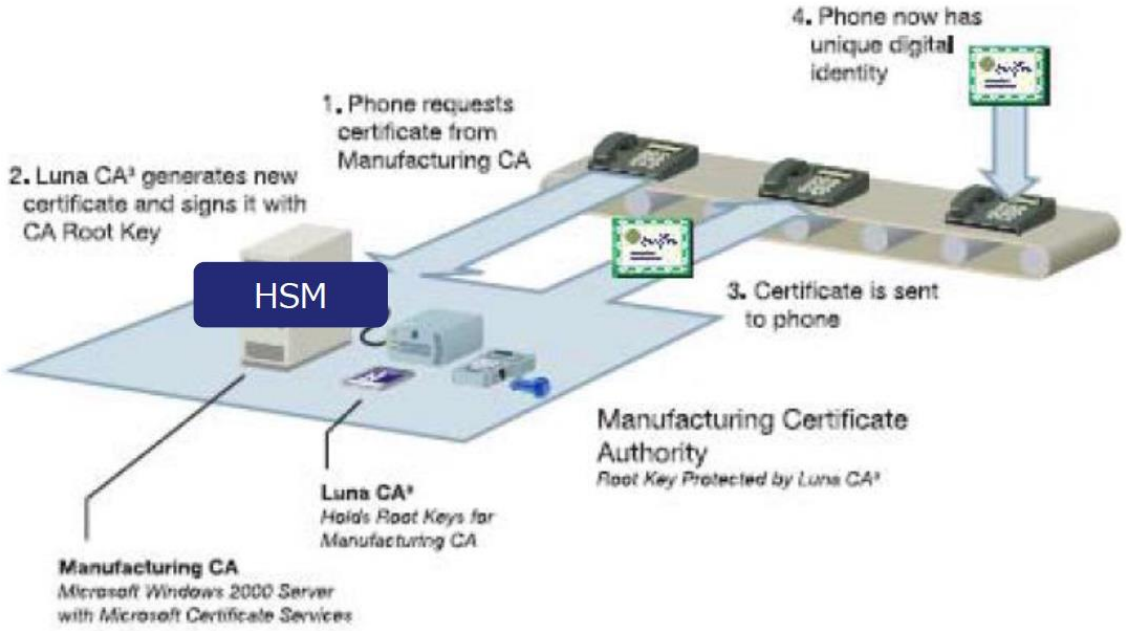
解決策

- HSMを活用して証明書発行/署名用鍵の保護を中央で管理するシステムを構築

HSMを利用する利点

- XX台のネットワーク型HSMを利用
  - HSMのサービス化
- HSM内で管理する鍵のポリシーを中央管理
  - 鍵の利用方法
  - 鍵の利用回数
  - 鍵は「決して」HSM外部に出さない

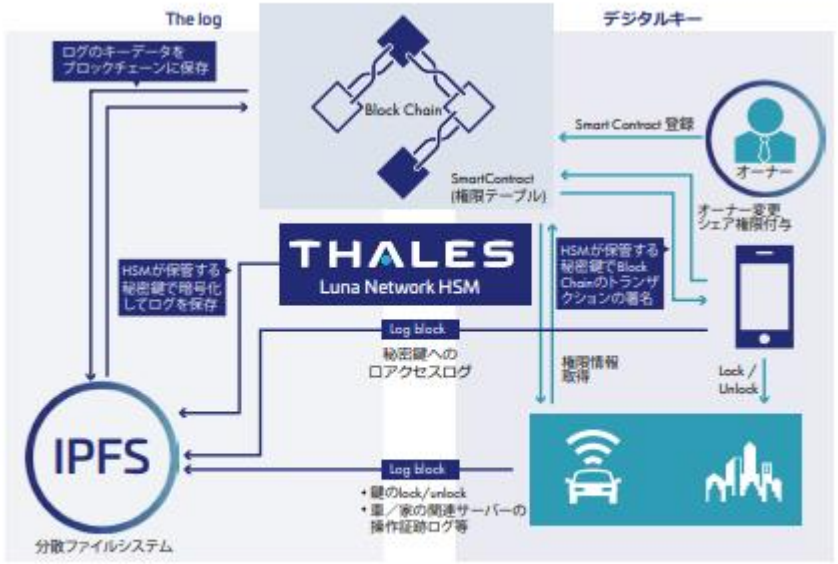
製造機器に電子証明書を発行して、委託工場での生産台数管理、出荷後の情報管理、各種メンテナンス等に利用



フリービット様事例

https://cpl.thalesgroup.com/sites/default/files/content/case_studies/field_document/2020-07/FreeBit_CS_A4_JP_v8.pdf

フリービット株式会社：ブロックチェーンとThales Luna Network HSMを組み合わせて、革新的なデジタルキー基盤を構築



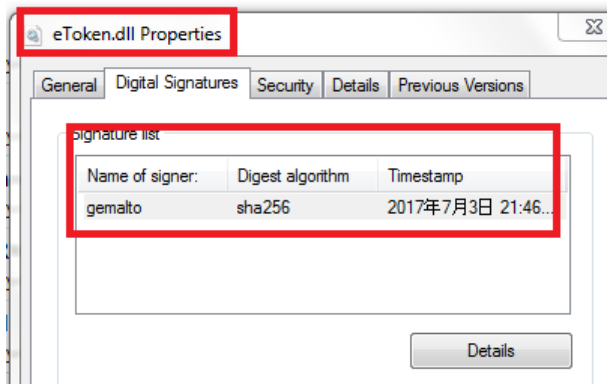
ブロックチェーンとLuna Network HSMを組み合わせたセキュリティな基盤で、革新的なデジタルキーシステム、およびオフチェーンのログ保管システムを構築

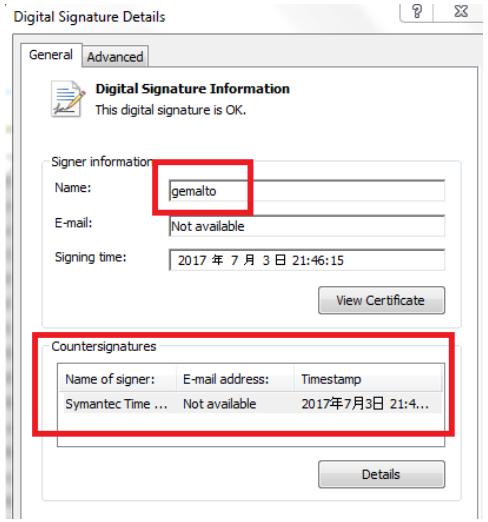
ソリューション

開発の初期段階では、鍵管理/利用において多数の独自APIを提供、また仮想化アプライアンスモデルをクラウド環境にも提供する鍵管理プラットフォーム「KeySecure」を使う予定で、プログラム開発と動作検証を進めました。開発途中でSafeNet Luna Network HSMに切り替えたのは、FIPS 140-2 Level 3のハードウエアによるセキュリティ、秘密鍵は決してハードウェア外に出さない運用、楕円曲線や各種必要な暗号アルゴリズムという各種セキュリティ機能、1台のHSMを複数HSMに仮想的に分割して利用できる機能(パーティション分割)またフリービット社独自でファームウェアに近い機能を開発できる拡張性を重視したためです。Luna Network HSMの開発には暗号デバイスの標準インターフェースであるPKCS#11を利用することですでに開発を進めていたウォレット機能を含めて、短期間で移行が完了。当初予定どおりにサービスをカットオーバーすることができました。

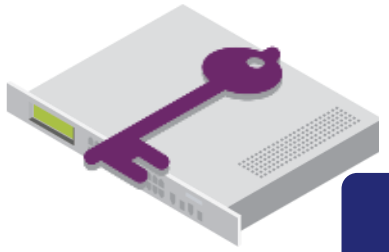
HSM活用例
タレス社内でも利用してます

実行されるコードが改ざんされていないことを保証するために「秘密鍵」が利用





コード署名用鍵/証明書



HSM

THALES

Thank you

Gracias شكرا لكم

धन्यवाद Merci

Danke 謝謝

ありがとうございました

付録

各種HSM
お客様ご要件により各種HSMをご用意

汎用HSM

https://cpl.thalesgroup.com/encryption/hardware-security-modules/network-hsms

- PKI
- 秘密鍵保護
- IOT
- ブロックチェーン
- PKCS#11
- TDE(DB暗号)
- カード発行
- 政府系/金融系システム指定

THALES

CipherTrust Manager

鍵管理＋暗号処理

- データ暗号
- PCIDSS
- トークナイゼーション
- ファイルサーバ暗号
- DBカラム単位暗号
- KMIP
- TDE(DB暗号)
- クラウドサービス鍵管理

電子資金決済処理

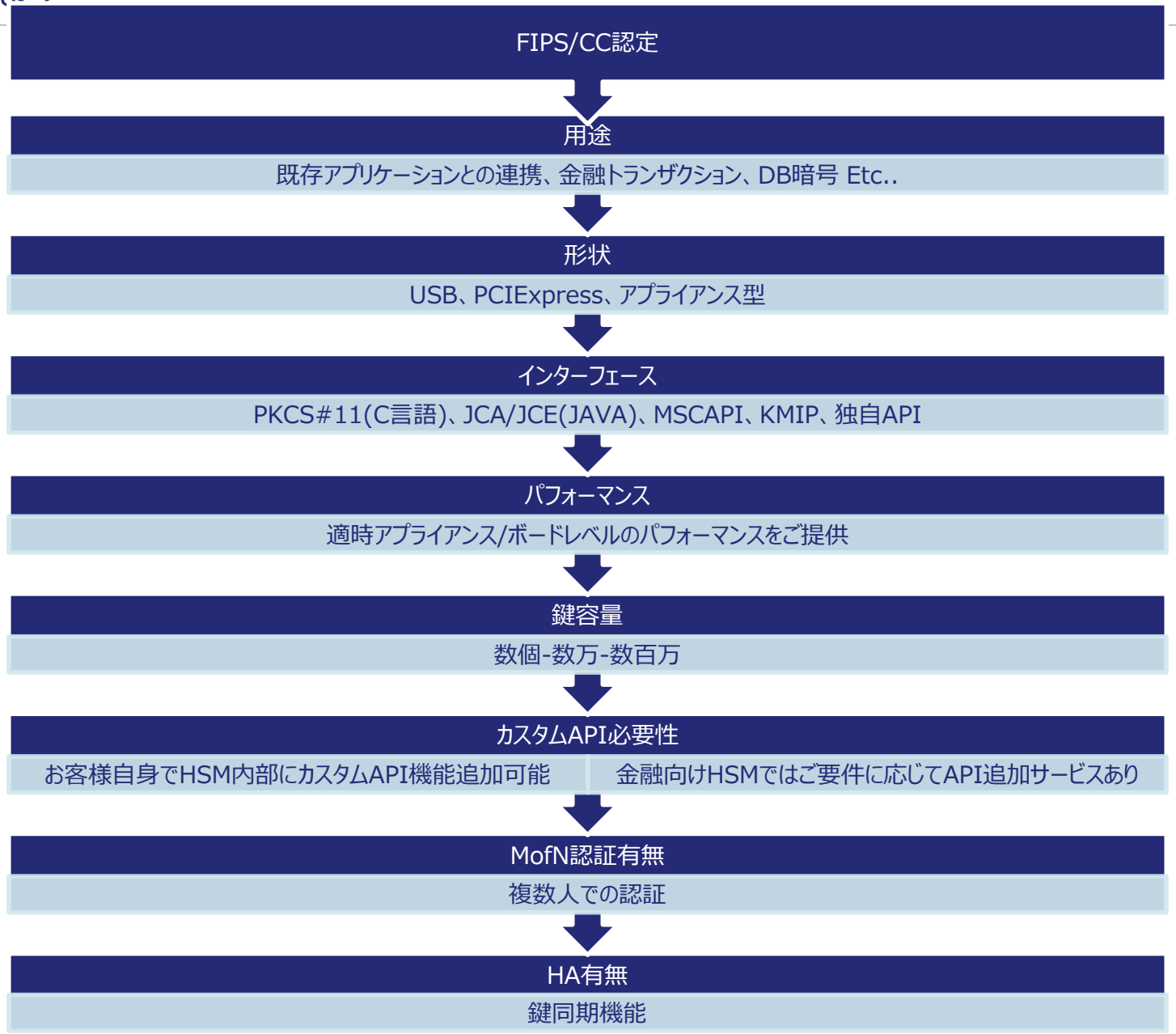
https://cpl.thalesgroup.com/encryption/hardware-security-modules/payment-hsms/payshield-10k

- オーソリ処理
- PCIHSM
- P2PE/DUKPT
- EMVカード発行
- 3D Secure

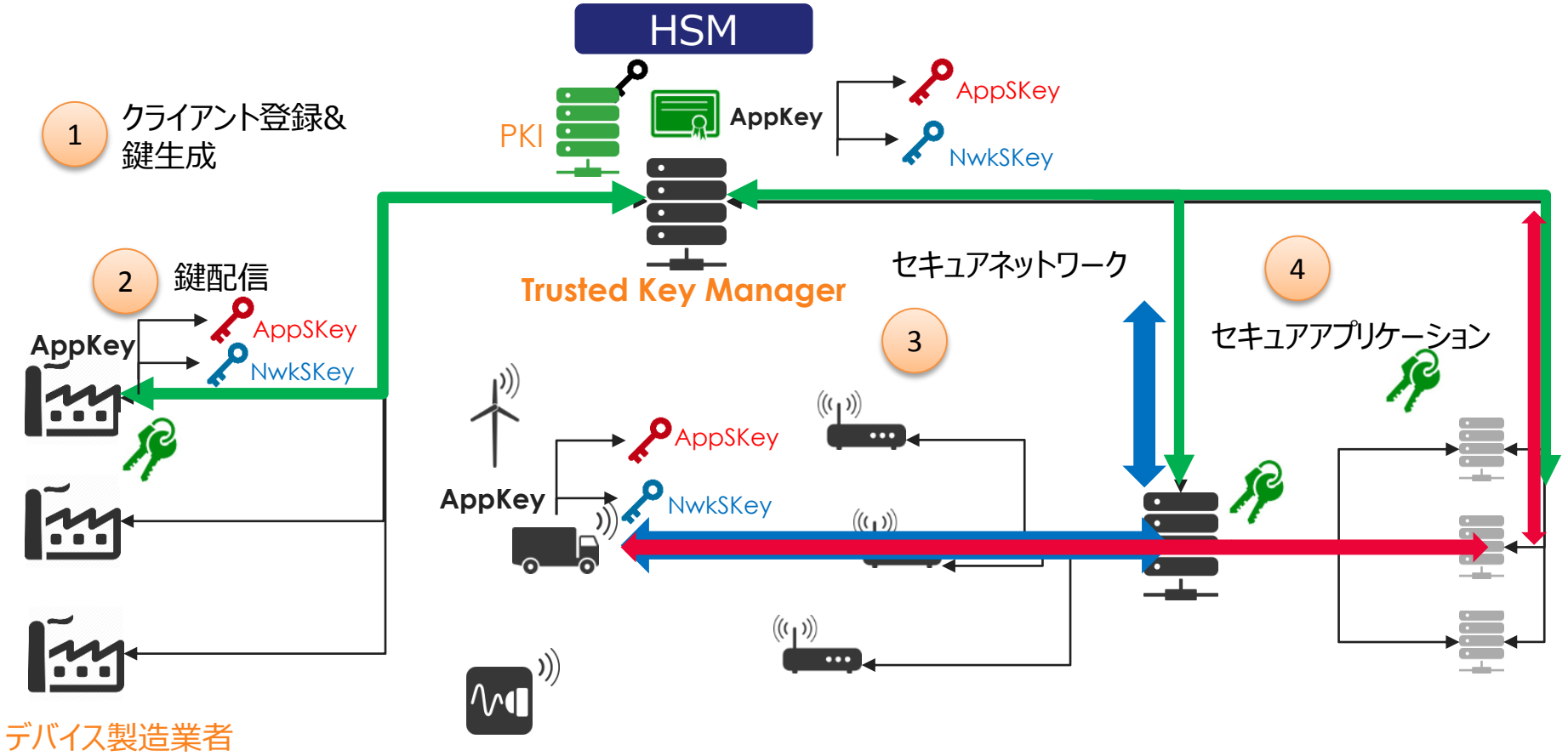
THALES

一般的なご要件確認項目

ここからお手伝いいたします



HSM活用例
Trusted Key Managerシステム構成例



- マスター鍵(AppKey)は、TKMでセキュアに保管
- デバイス製造者、ネットワーク提供者、サービスプロバイダーには開示されない
- ネットワーク提供者がアプリケーションレイヤーのデータのアクセス不可

22

Thales Luna Network HSM
各機材例

SafeNet Luna Network HSMハードウェア

- 電源ケーブル2本

クライアントライセンス

- SafeNet Luna Network HSMに接続するサーバごとに必要

バックアップHSM

- オプション

PED

- 2要素認証モデルに必要

PED鍵

- 2要素認証モデルに必要

POC支援

- 製品QA対応/日本語簡易ハンズオンガイド提供

クラウドHSMサービスご紹介

正式名称：
Data Protection On Demand(DPoD)

暗号＋鍵管理の顧客要望の高まり → クラウド利用拡大には「顧客自身が鍵管理する仕組み」が必要 → クラウドサービス事業者によるクラウドHSM → Gemalto(当時)が2018年からクラウドHSMサービス開始

https://azure.microsoft.com/ja-jp/services/azure-dedicated-hsm/

アプリケーションを Azure に簡単に移行する

Gemalto とのパートナーシップにより開発された SafeNet Luna Network HSM 7 Model A790 クラウドベース HSM は多くのアプリケーションと互換性があり、従来型またはカスタムのオンプレミスのアプリケーションから Azure への簡単な移行を可能にします。オンプレミスのアプリケーションが Azure で機能するために必要な変更はわずかなので、時間を節約できます。ハイブリッド機能を利用すると、従来のまたはカスタムのアプリケーションをオンプレミスの Gemalto HSM でも Azure でも実行できます。さらにセキュリティを強化するには、キーのコピーを Gemalto HSM に保持します。

https://www.ibm.com/cloud/hardware-security-module/

What is IBM Cloud HSM 7.0?

IBM Cloud Hardware Security Module (HSM) 7.0 from Gemalto protects the cryptographic infrastructure of some of the most security-conscious organizations in the world by securely managing, processing and storing cryptographic keys inside a tamper-resistant, tamper-evident device. With IBM Cloud HSM 7.0, you can solve complex security, compliance, data sovereignty and control challenges associated with migrating and running workloads on the cloud.

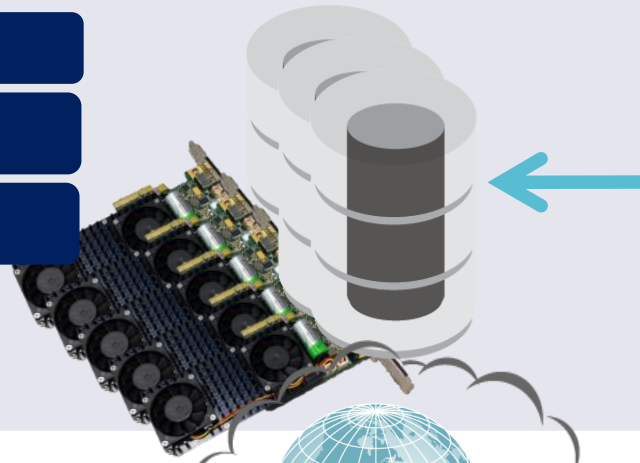
SafeNet Data Protection On Demand
クラウドHSMサービス

Thalesが提供

SLAあり 99.95%

バックアップ/冗長化

FIPS140-2 L3



HSM運用管理

サービスモニタリング

HSM設置

バックアップ

可用性確保

システムメンテナンス

HSMアクセス情報連携

お客様作業範囲

HSM管理者

lunacm:>

①HSMポリシー設定

②HSMユーザ設定

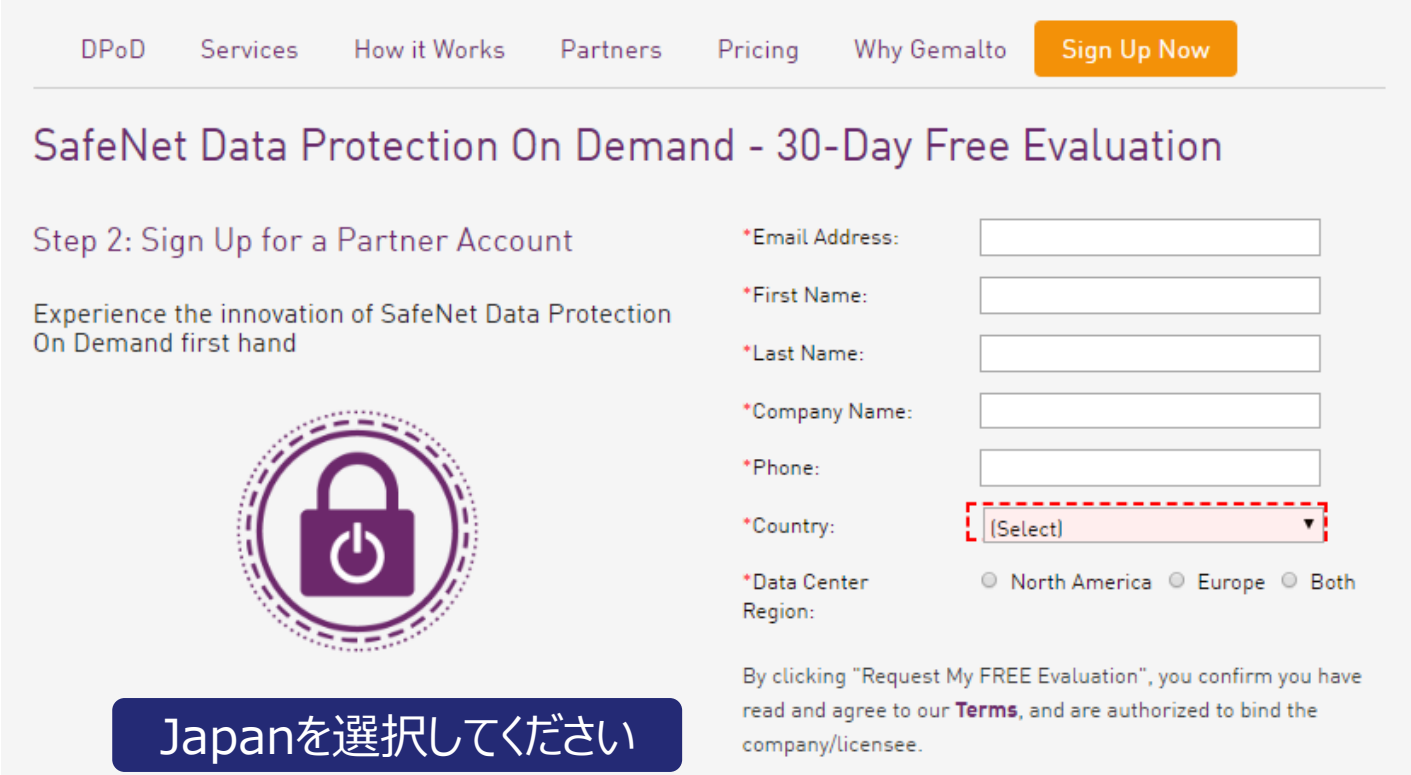
DPoDクライアントインストール

③アプリケーション/開発/インテグレーション

アプリケーションチーム

SafeNet Data Protection On Demand
トライアルサイト

- https://safenet.gemalto.com/data-protection-on-demand/marketplace/
- 無料半日トレーニング
- クイックスタートガイドご提供



ご意見ご要望
お待ちしております

鍵管理検討される背景

検討した際の課題

HSMベンダに期待すること

- ホワイトペーパー？海外事例？機能？

舟木 康浩
タレスDIS CPLジャパン株式会社
Yasuhiro.Funaki@thalesgroup.com