THALES
Building a future we can all trust

eSIMの動向とセキュリティ活用

タレスDISジャパン株式会社
モバイルコネクティビティソリューションズ
フィールドマーケティング
米沢正雄

THALES GROUP LIMITED
DISTRIBUTION

タレスグループ: 5つのコアアクティビティ

OPEN

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2018 All rights reserved.

THALES
Building a future we can all trust

デジタルアイデンティティ & セキュリティ:
信頼できるコネクティビティを人とものに

ソリューション

- 人とデバイスの認証
- eSIM サブスクリプションマネージメント
- 本人確認
- クラウドセキュリティ
- 分析とAI

顧客

- MNO/MVNO
- デバイスメーカー
- サービスプロバイダー
- 自動車メーカー
- 公共交通機関
- インテグレーター
- 政府機関

最初のGSM規格から30年以上にわたり、テレコム業界の形成に貢献

世界で450以上のモバイルオペレーターに製品・ソリューションを提供

270以上の案件でタレスのeSIMプラットフォームが採用

THALES
Building a future we can all trust

アジェンダ

SIMからeSIM, iSIMへ

- eSIM(eUICC)のこれまで
- eSIM(eUICC)の技術的な拡張

セキュリティ活用

- GSMA IoT SAFE

さらなる発展へ

- ETSI Smart Secure Platform (SSP)

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2018 All rights reserved.

THALES
Building a future we can all trust

THALES
Building a future we can all trust

eSIM(eUICC)のこれまで

THALES GROUP LIMITED
DISTRIBUTION

セキュアエレメントとは

- セキュアエレメント(SE)とは、耐タンパー性のあるプラットフォームで、信頼される管理者により定義されたルールとセキュリティ要件に従い、セキュアなアプリケーションと暗号データ(鍵管理など)を扱う

- 2018年には、62億個のGlobalPlatform仕様に準拠したセキュアエレメントが発行

スマートカード(決済、ID、…)

(e)UICC

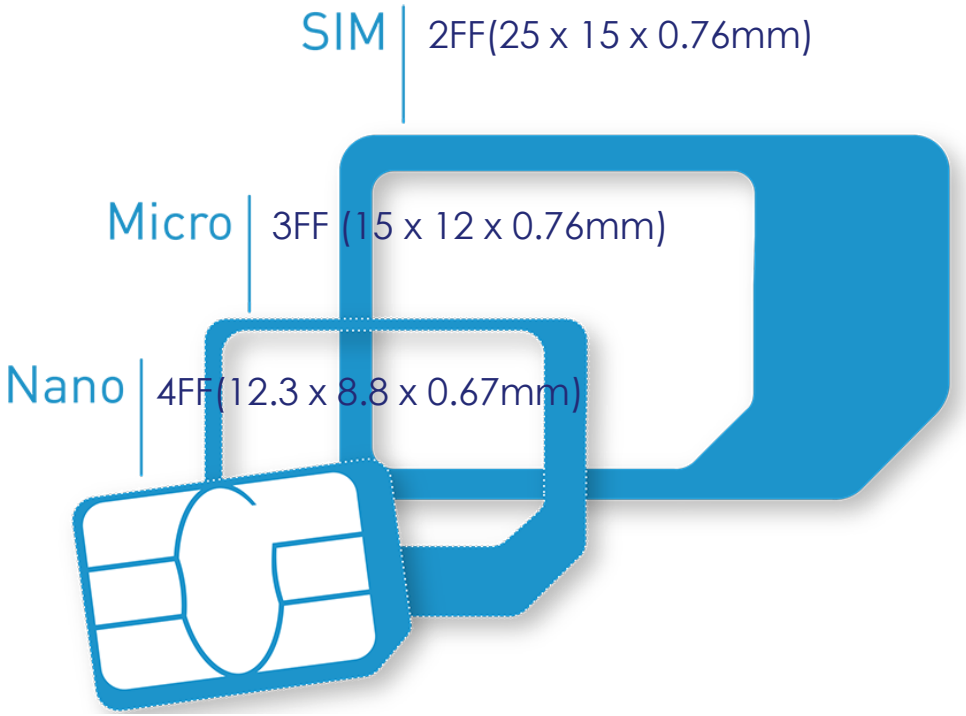
エンベデッドセキュアエレメント(eSE)

GLOBALPLATFORM®
THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

https://globalplatform.org/resource-publication/introduction-to-secure-elements/

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2018 All rights reserved.

SIMカードから埋め込みSIMへ



M2M機器からの要求

- 耐久性
  - 温度(-40～105℃)
  - 湿度
  - 振動
- 信頼性
  - 10年+
- 小型化

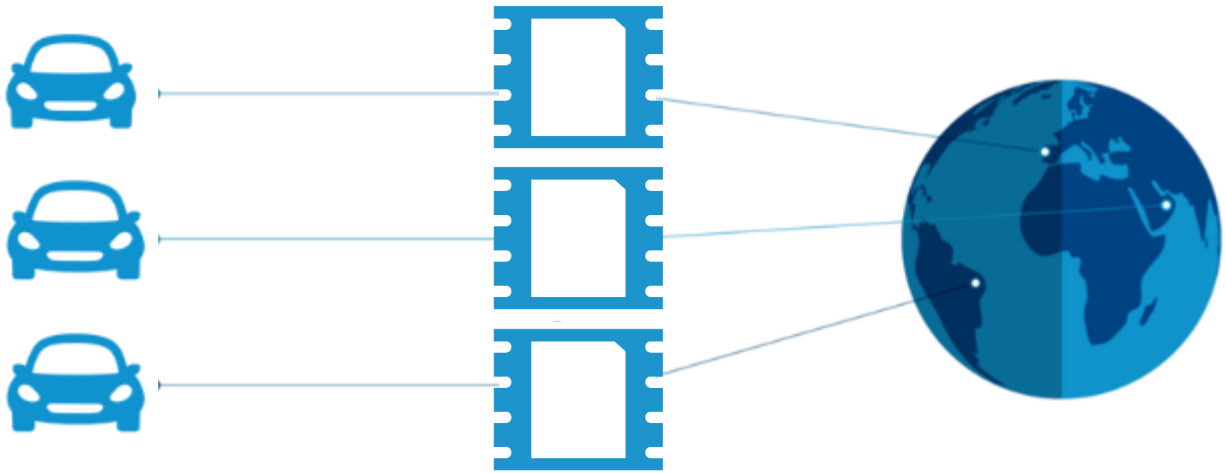
MFF2
(6mm x 5mm x 0.67mm)
ETSI TS 102 671 R9 (2010)

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2018 All rights reserved.

THALES
Building a future we can all trust

埋め込みSIMによる物流の複雑化

複数の製品に対して、複数のMNOプロファイルを搭載し、複数のロケーションに展開 (複数のSKU)



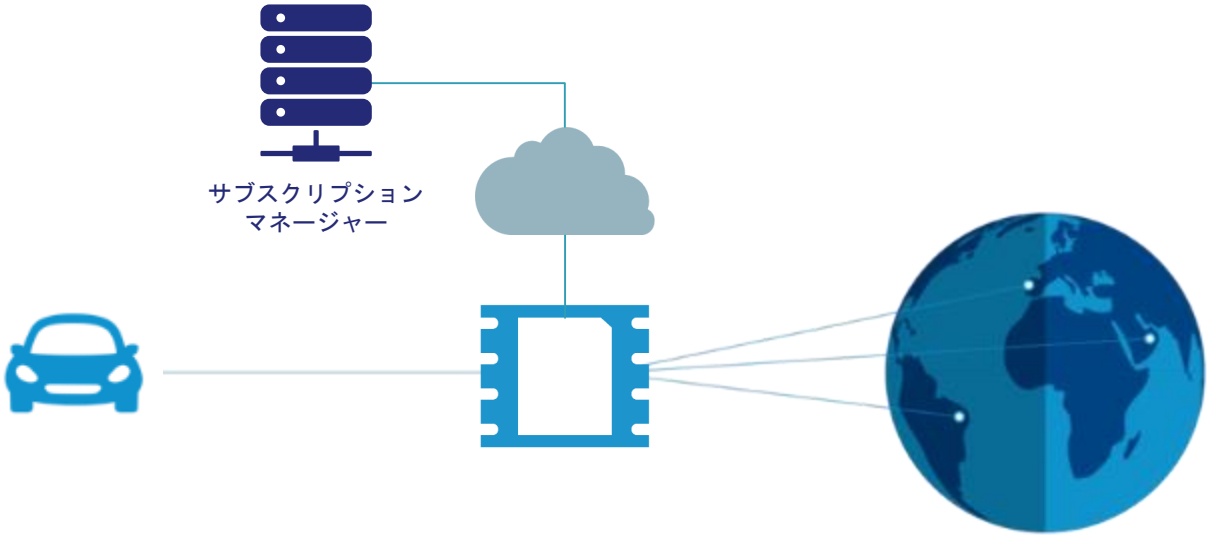
This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2018 All rights reserved.

OPEN

THALES
Building a future we can all trust

eSIM リモートプロビジョニング

一つの製品を使用開始時にパーソナライズすることで、どこでも使えるように



eSIM: 物理的に埋め込まれたSIM
eUICC: リモートプロビジョニング可能なSIMカード(埋め込み or リムーバブル)

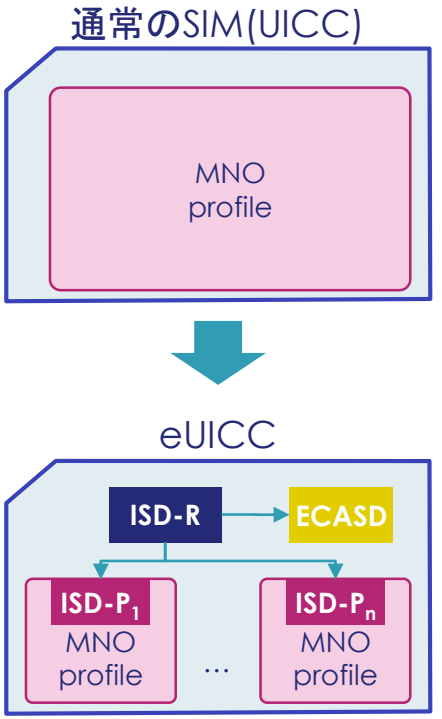
This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2018 All rights reserved.

THALES
Building a future we can all trust

eUICC: 論理アーキテクチャーの進化

GSMAによる標準化

- GlobalPlatform仕様で定義されたセキュリティドメイン(SD)
  - **ISD-R**: ISD-Pの作成とライフサイクル管理
  - **ISD-P**: 個々のプロファイルを格納するセキュアコンテナー。MNOは自分のプロファイルにだけOTAアクセス可能
  - **ECASD**: eUICC固有の証明書を格納し、サーバー証明書の検証を行う
- セキュアチャネルプロトコル(SCP)による相互認証と暗号化
- サブスクリプションマネージャーによるリモートプロビジョニング

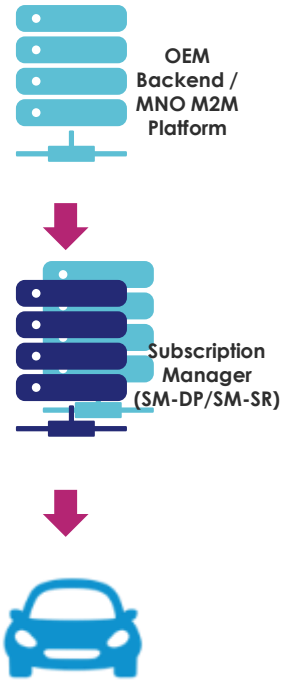


ISD-**R**: Issuer Security Domain **Root**
ISD-**P**: Issuer Security Domain **Profile**
ECASD: eUICC Controlling Authority SD

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2018 All rights reserved.

M2Mからコンシューマーデバイスへ

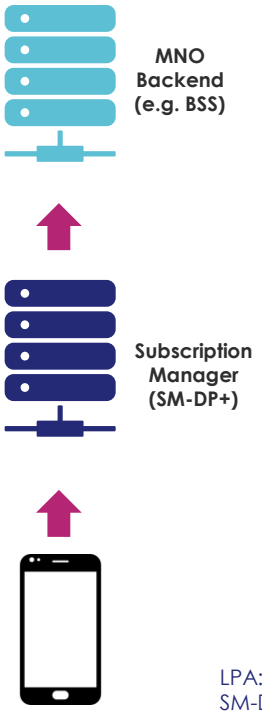
M2Mデバイスアプローチ (Push)



- OEMバックエンド・M2Mプラットフォームからのプッシュ(SMS)によるサブスクリプションマネージメント
- ブートストラッププロファイルにより、規定のSM-SRと接続
- MNOプロファイルを管理するSM-DP
- 必要に応じたSM-SRの変更

SM-DP: Subscription Manager Data Preparation
SM-SR: Subscription Manager Secure Routing

コンシューマーデバイスアプローチ (Pull)



- LPAアプリケーションから、ユーザープルによるサブスクリプションダウンロード
- ユーザーが選択した任意のSM-DP+への接続
- イニシャルコネクティビティとしてデバイスのネットワーク機能(WiFiなど)を利用可能
- SM-DSを用いたシンプルはユーザーエクスペリエンスも実現可能

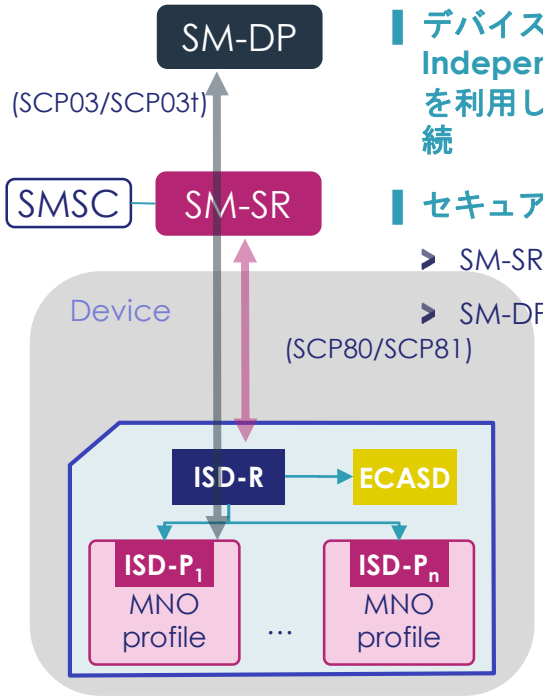
LPA: Local Profile Assistant
SM-DP+: Subscription Manager Data Preparation+
SM-DS: Subscription Manager Discovery Server

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2018 All rights reserved.

THALES
Building a future we can all trust

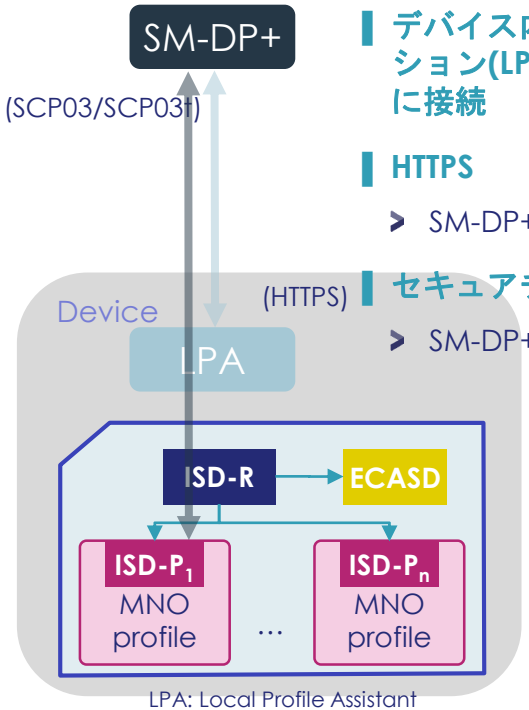
それぞれのセキュリティアーキテクチャー

M2Mアーキテクチャー



- デバイスのBIP (Bearer Independent Protocol)を利用してサーバーに接続
- セキュアチャネル
  - SM-SR⇔eUICC
  - SM-DP⇔eUICC

コンシューマーデバイスアーキテクチャー



- デバイス内のアプリケーション(LPA)がサーバーに接続
- HTTPS
  - SM-DP+⇔LPA
- セキュアチャネル
  - SM-DP+⇔eUICC

LPA: Local Profile Assistant
SM-DP+: Subscription Manager Data Preparation+

SM-DP: Subscription Manager Data Preparation
SM-SR: Subscription Manager Secure Routing
SCP: Secure Channel Protocol

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2018 All rights reserved.

eSIM (eUICC) の普及状況と予想

eSIMの現在(Trusted Connectivity Alliance, Mar 2021)

- 2020年には、**3.09億**のeSIMが出荷(前年比83%増加)
- プロファイルダウンロード回数は前年比**300%**の増加
- 累計**687**のサブスクリプションマネージャーが稼働(前年比154%増加)
- 従来のSIMカード: 48億個出荷

eSIMの普及予想 (GSMA Intelligence, June 2020)

- 2025年までに、世界で**20~30億**のモバイル回線がeSIMを使用すると予想(スマートフォンの**35%**に相当)
- COVID-19の影響でデジタル化が加速し、さらにeSIMの利用が進む可能性

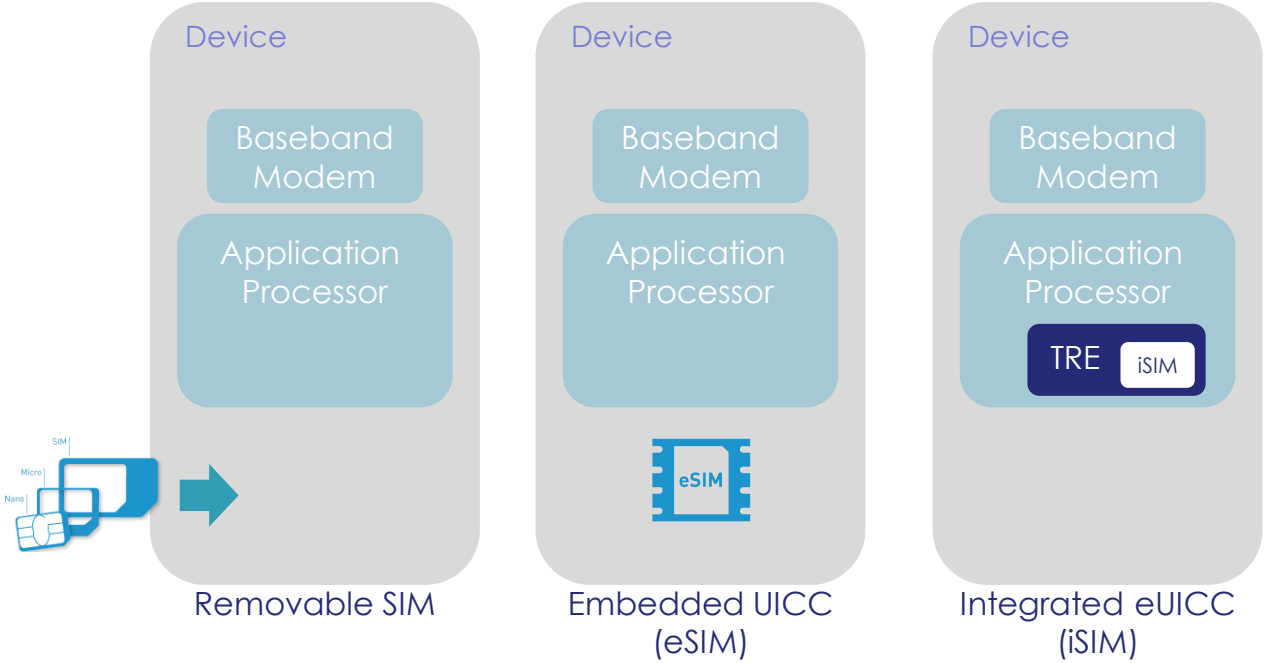
This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2018 All rights reserved.

THALES
Building a future we can all trust

eSIM(eUICC)の技術的な拡張

THALES GROUP LIMITED
DISTRIBUTION

Integrated eUICC (iSIM): SoCに統合されたeUICC



SoC: System on Chip
TRE: Tamper Registrant Element

iSIMの利点

- シンプルな実装、基盤スペースの有効活用、BOMの削減、低電力消費
- eSIMと同じハードウェアベースのセキュリティ(TRE)と、既存のeSIMエコシステムの活用(SM-DP+)

Integrate eSIMのため、Qualcomm Technologiesと協業 (2018/5/29)

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2018 All rights reserved.

eSIM + eSE = “コネクティッド eSE” (Thales)

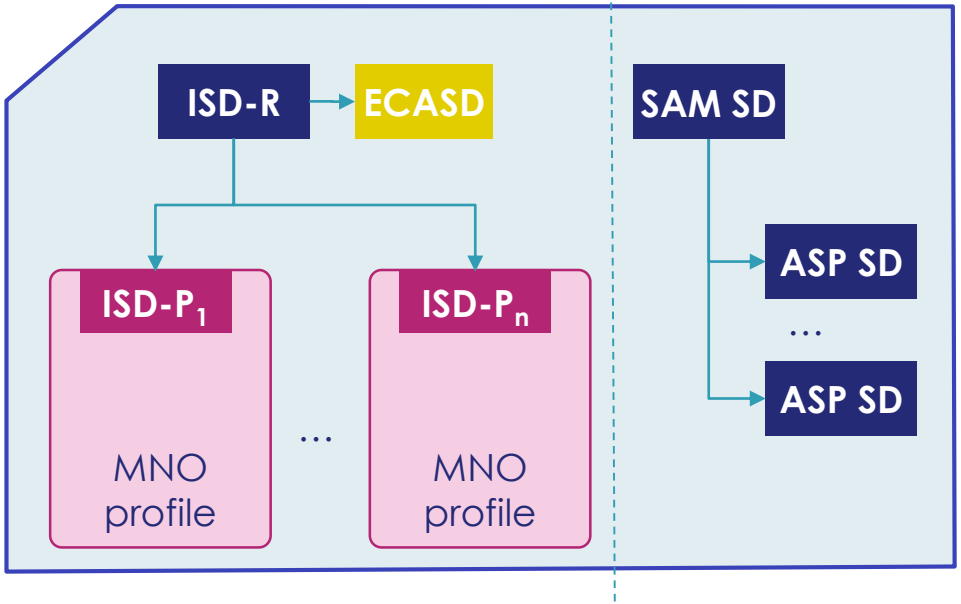
- 一つのチップ上で、eSEとeSIM機能の機能を統合
- 2つのユースケース間でクリアな隔離を提供するセキュアなサイロ
- ペイメント、トランスポートなどの既存のユースケースに加えて、デジタルキーやeIDの新たなセキュアユースケースを見込む
- タレスのSM-DP+と世界の主要MNOとの相互接続の経験を通して検証されたeSIMのサポート

タレスの次世代シングルチップ・ソリューションをサムスンの最新フラッグシップ・スマートフォンに搭載 (2020/6/16)

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2018 All rights reserved.

GSMA Secured Applications for Mobile (SAM)

- eUICC内で様々なセキュアアプリケーションを利用を可能に
- eUICC内のMNOプロファイルとは独立して動作
- **SAM SM(TSM)による管理**
- **ユースケース**
  - バンキング・ペイメント
  - 交通系
  - eID/mDL
  - GSMA IoT SAFE



ASP: Application Service Provider
SAM SM (SAM Service Manager)

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2018 All rights reserved.

THALES
Building a future we can all trust

eSIMのセキュリティ活用

GSMA IoT SAFE

THALES GROUP LIMITED
DISTRIBUTION

IoTデバイスとクラウド間のセキュリティの課題

クラウドとの通信におけるセキュリティ

- 認証、整合性、機密性→クライアント・サーバー証明書による相互認証

デバイスへの証明書のプロビジョニング

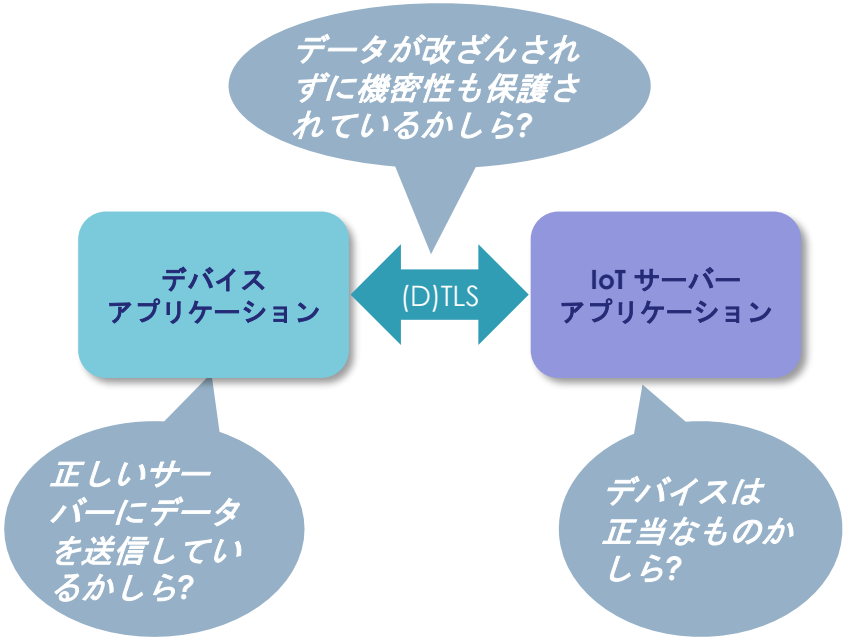
- デバイス製造時には、サービス・プロバイダーがどのクラウドサービスを使うかは不明

証明書のライフライクル管理

- デバイスが既にフィールドに設置済みの場合は?

証明書の格納場所

- 耐タンパーなセキュアエレメントの必要性

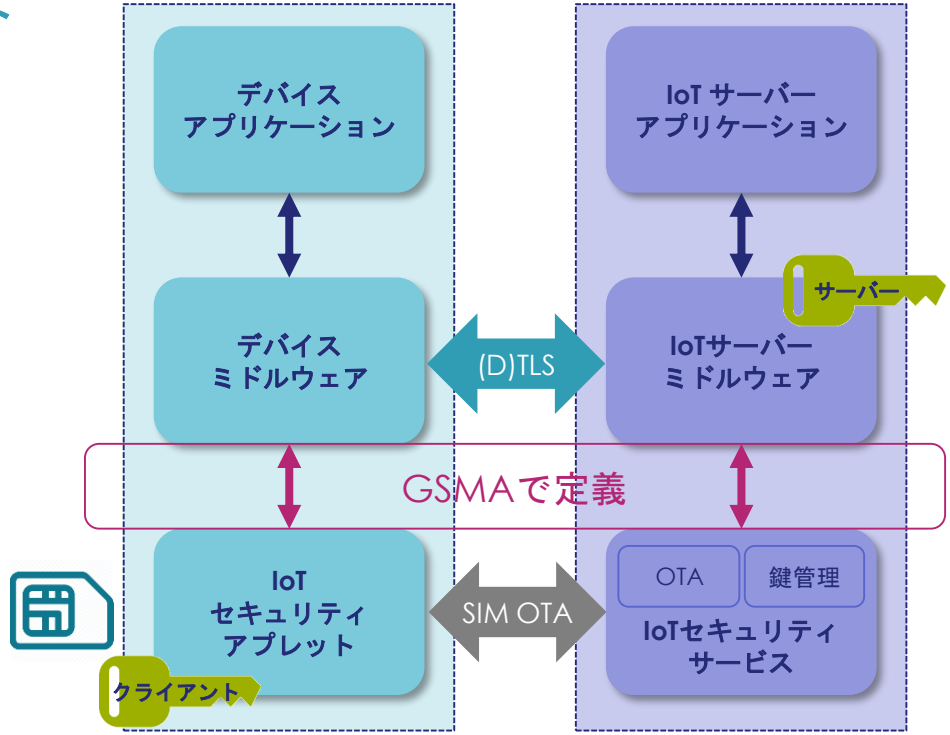


This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2018 All rights reserved.

THALES
Building a future we can all trust

GSMA IoT SAFE (IoT SIM Applet For Secure End-to-End Communicaiton)

- IoTデバイスが、クラウドとセキュアな通信(TLS)を確立するのための鍵の格納と、セキュリティサービスのためにSIMカードアプレットを活用
- アプレット管理にはSIM OTAサーバーが利用可能
- アプリケーションとは別チャネル(OTA)を利用し、鍵・証明書のセキュアなゼロタッチプロビジョニングが可能



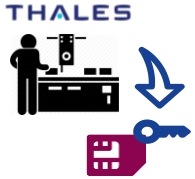
This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2018 All rights reserved.

OPEN

THALES
Building a future we can all trust

IoTクラウドとのセキュアな通信のためのフロー

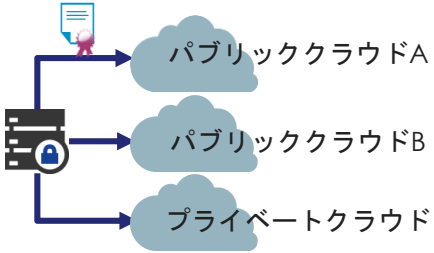
1 デバイスIDの生成



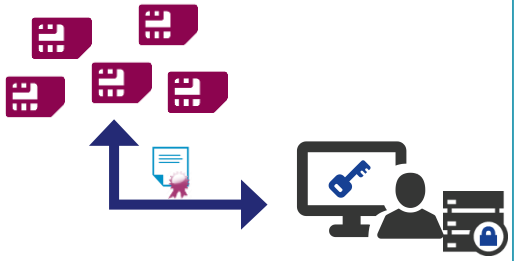
- SIM発行時

- OBKG
(オンボード鍵生成)

2 IoTクラウドへのデバイスIDをプロビジョニング



3 デバイスIDのライフサイクル管理



- 生成: 追加のID
- 失効: IDの無効化
- 更新: 証明書の更新
- 変更: クラウドプロバイダーの変更

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2018 All rights reserved.

OPEN

THALES
Building a future we can all trust

THALES
Building a future we can all trust

さらなる発展へ

ETSI Smart Secure Platform (SSP)

THALES GROUP LIMITED
DISTRIBUTION

ETSI Smart Secure Platform (SSP)

市場の新たな要望に答えるため、2015年10月に最初の議論

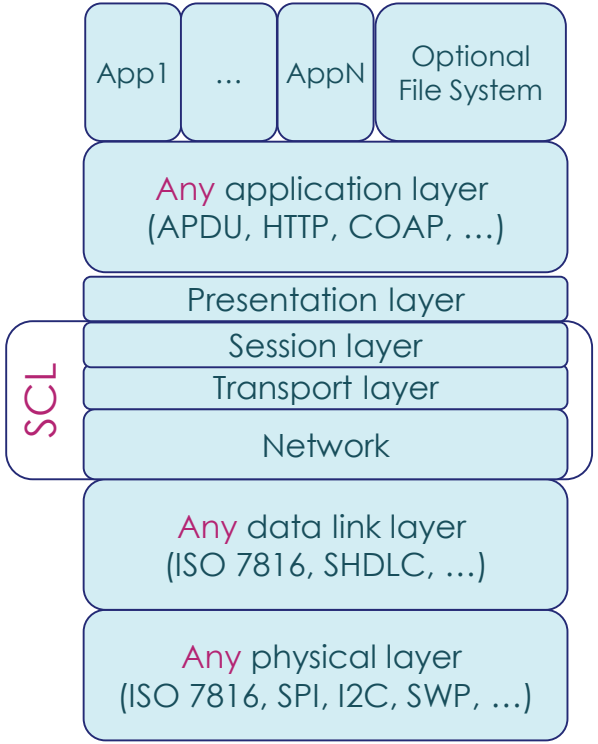
- 柔軟性・多用途性・費用効果・セキュリティ

特徴

- モジュラープラットフォーム
- インターフェースの多様化(ISO7816, SPI, I2C, etc.)
- 共通のレイヤー: SSP Common Layer (SCL)

複数のクラス

- Integrated SSP (iSSP)
- Embedded SSP (eSSP)
  - Type 1: (シングルOS)
  - Type 2: Primary/Secondary Platformをサポート
- Removable SSP (rSSP)

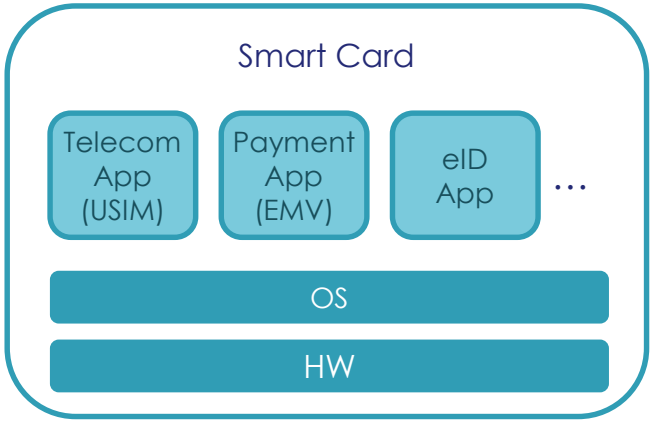


SSP Protocol Stack
(ETSI TS 103 465)

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2018 All rights reserved.

THALES
Building a future we can all trust

これまでのスマートカードにおけるマルチアプリケーション実現の課題



ハードウェアに依存した実装

異なるステイクホルダー

- MNO、ペイメントサービスプロバイダー、政府、…

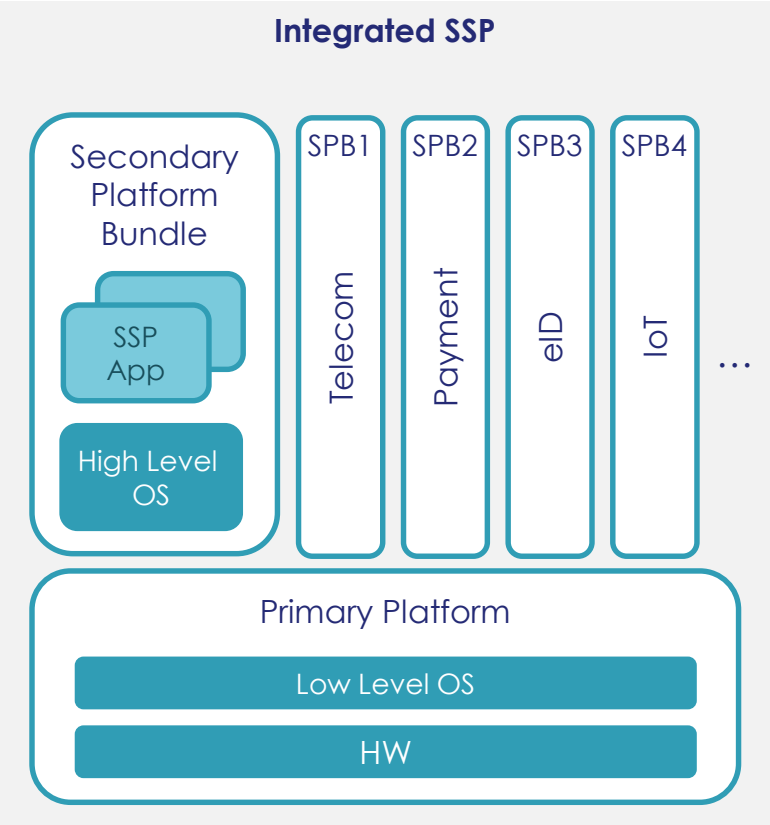
異なる認定スキーム

複雑なライフサイクル管理

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2018 All rights reserved.

THALES
Building a future we can all trust

Integrated SSP



Primary Platform

- HWとHW技術に依存するソフトウェア(ローレベルOS、通信サービス)

Secondary Platform Bundle (SPB)

- HWに依存しないハイレベルOSとアプリケーション
- 複数のSPBを搭載可能だが、ある時点でアクティブにできるSPBは一つ
- Telecom Bundle: 3GPPに準拠したバンドル →(e.g. eUICC)

SSP Application

- SSPで動作するアプリケーション(アプレット)

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2018 All rights reserved.

まとめ

eSIMの標準化と普及

- M2Mからコンシューマーデバイスへの普及が拡大
- IoTデバイスへの適用
- iSIM(iUICC)の導入

eSIMの技術的な拡張による利用用途の拡大

- GSMA SAM, ETSI SSPにより、eSIMを複数の用途で利用することがより柔軟に

eSIMの活用

- GSMA IoT SAFE
- eSEとの統合

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2018 All rights reserved.