THALES
Building a future we can all trust

資料４－２

スイッチング円滑化タスクフォース資料

GSMA eSIM セキュリティ

タレスＤＩＳジャパン株式会社

2021/1/27

タレスグループ: 5つのコアアクティビティ

OPEN

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**

240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

eSIMの現在と、その普及の加速

eSIMとは

- モバイルサブスクリプション情報を格納する、**耐タンパー**なセキュアチップ
- デバイスの小型化・防水性能の向上や、MNOロジスティクスの簡潔化、ユーザーエクスペリエンスのデジタル化などを可能に

MFF2
(5mm x 6mm)

WLCSP

eSIMの現在と普及予想 (GSMA Intelligence, June 2020)

- 世界60カ国・158以上のMNO/MVNOがスマートフォン向けのサービスを提供(2020年6月)
- 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

GSMA Intelligence

eSIMについて

本資料は、GSMAにより仕様化された「コンシューマーデバイス」向けリモートSIMプロビジョニング仕様についての説明

- SGP.21: eSIM Architecture Specification
- SGP.22: eSIM Technical Specification

SM-DP+:

- プロファイルの管理・ダウンロードを行うサーバー

eUICC:

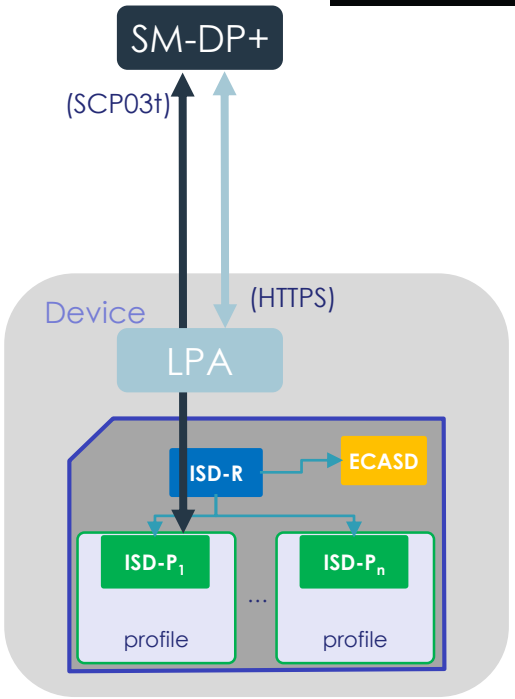
- リモートプロビジョニング可能なUICC (*物理的な形状は問わない)

LPA (Local Profile Assistant)

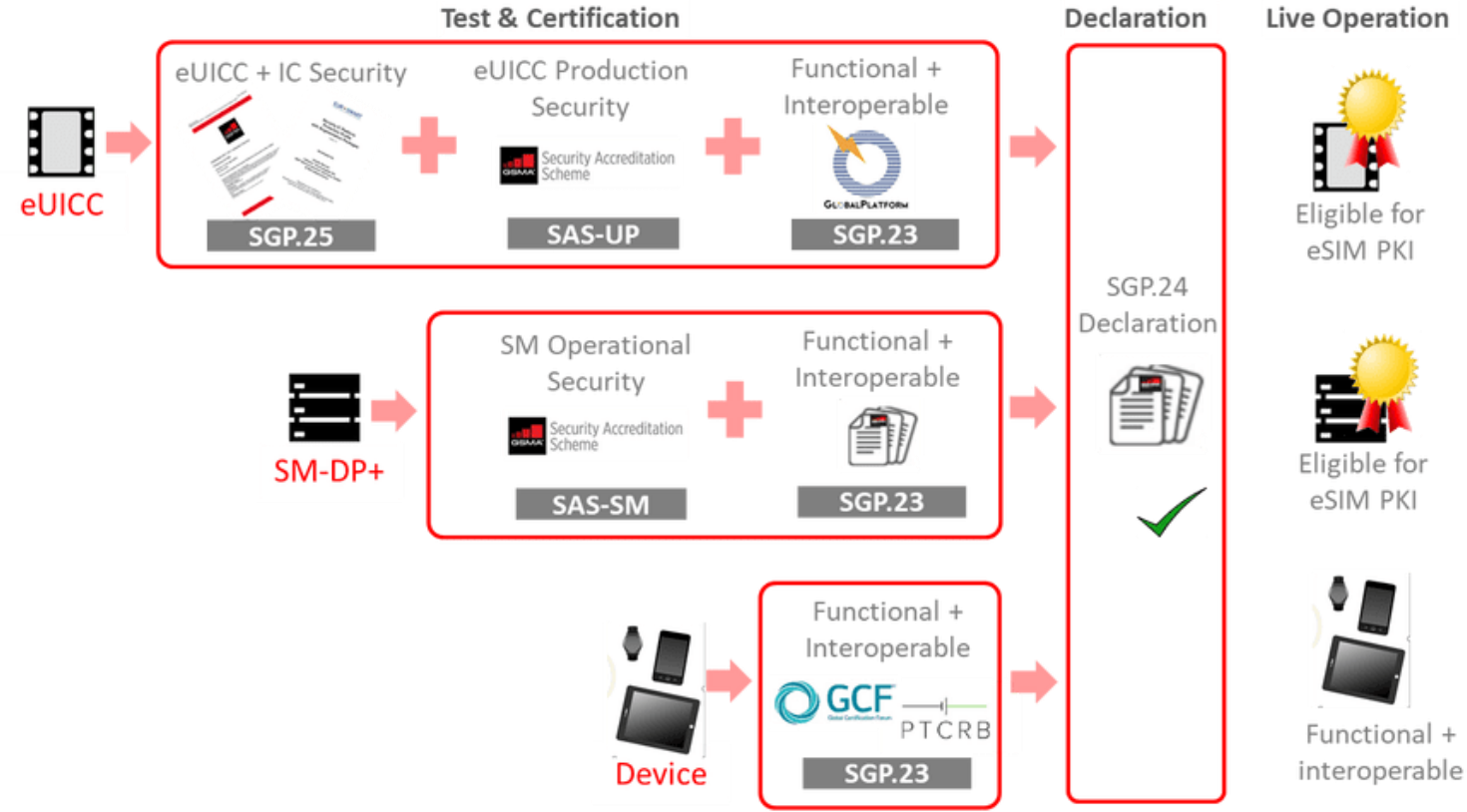
- 暗号化されたプロファイルをeUICCにダウンロードし、エンドユーザーがプロファイルの管理をするためのデバイス側の機能

プロファイル

- ネットワーク認証鍵を含むMNOデータセット



GSMAによる厳格なコンプライアンスプロセス

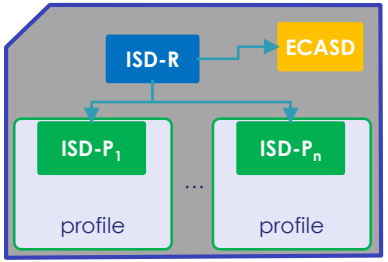


Source: https://www.gsma.com/esim/compliance/

MNOプロファイルを保護するためのeUICCセキュリティ

eUICCのセキュリティメカニズム

- 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



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

eUICCのセキュリティ評価

- ハードウェア
  - Common Criteria EAL4+ (AVA_VAN.5 and ALC_DVS.2)を取得
- OSプラットフォーム
  - GSMA SGP.25/PP-0100(EAL4+)のセキュリテイ目的を満たしていることの評価を、スマートカードドメインで資格を持つSOG-ISラボで実施*

AVA_VAN.5: 脆弱性評価
ALC_DVS.2: 開発セキュリティ

*2019年末からの暫定スキーム。2022年からは正式スキームに移行し、Common Criteria EAL4+(AVA_VAN.5 and ALC_DVS.2)取得(GSMA SGP.25/PP-0100)

サーバー側のセキュリティ: GSMA Security Accreditation Scheme

eUICCプロファイル管理のための環境・プロセスに対するセキュリティ認定スキーム

- SAS-SM (サブスクリプションマネージャー)
  - Secure Routing
  - Data Preparation
  - Data Preparation+
  - Data Centre Operations & Management
  - Discovery Service
- SAS-UP (UICC Production)
  - Generation of data for personalization (UICC/eUICC)
  - Personalisation
  - Management of PKI Certificate
  - Post personalisation packaging

GSMA Security Accreditation Scheme

論理・物理セキュリティ要件を定義

- 共通要件
  - 人事のセキュリティ(スクリーニングチェックのポリシーの定義、教育、など)
  - 物理的なセキュリティ(アクセスコントロール、CCTV、内部監査、など)
  - …
- サブスクリプションマネージャー要件
  - 暗号計算にはFIPS14-2 Level3認定の**HSM**を使用
  - 証明書や鍵の管理のオペレーションには**デュアルコントロール**が必要
  - 許可されたスタッフのみがアクセスでき、物理的なコントロールもされている**High Security Area**
  - …

監査による認定制度

- 約5日間のDry Auditにより**Provisional Certification**の取得
- 決められた期間の実運用開始後、2日間のWet Auditを経て、**Full Certification**を取得
- 2年ごとのリニューアル

GSMA SAS取得拠点リスト

https://www.gsma.com/security/sas-accredited-sites/

SAS-UP Accredited sites.

Supplier	Site	Certification Scope				Valid to:	Cert.
		Generation of data for personalisation	Personalisation	Management of PKI certificates	Post personalisation packaging		
Thales DIS France [1]	Pont Audemer, France	UICC, eUICC	C E	GSMA PKI	C	Apr 2021	
Thales DIS Mexico S.A. de C.V. [1]	Cuernavaca, Mexico	UICC, eUICC	C	GSMA PKI	C	Aug 2021	
Thales DIS (Shanghai) Co., Ltd. [1]	Shanghai, China	UICC, eUICC	C E	GSMA PKI			
Thales DIS Sp. z o. o [1]	Tczew, Poland	UICC	C	-			
Thales DIS USA, Inc. [1]	Montgomeryville, USA	UICC, eUICC	-	GSMA PKI			

SAS-SM Accredited sites.

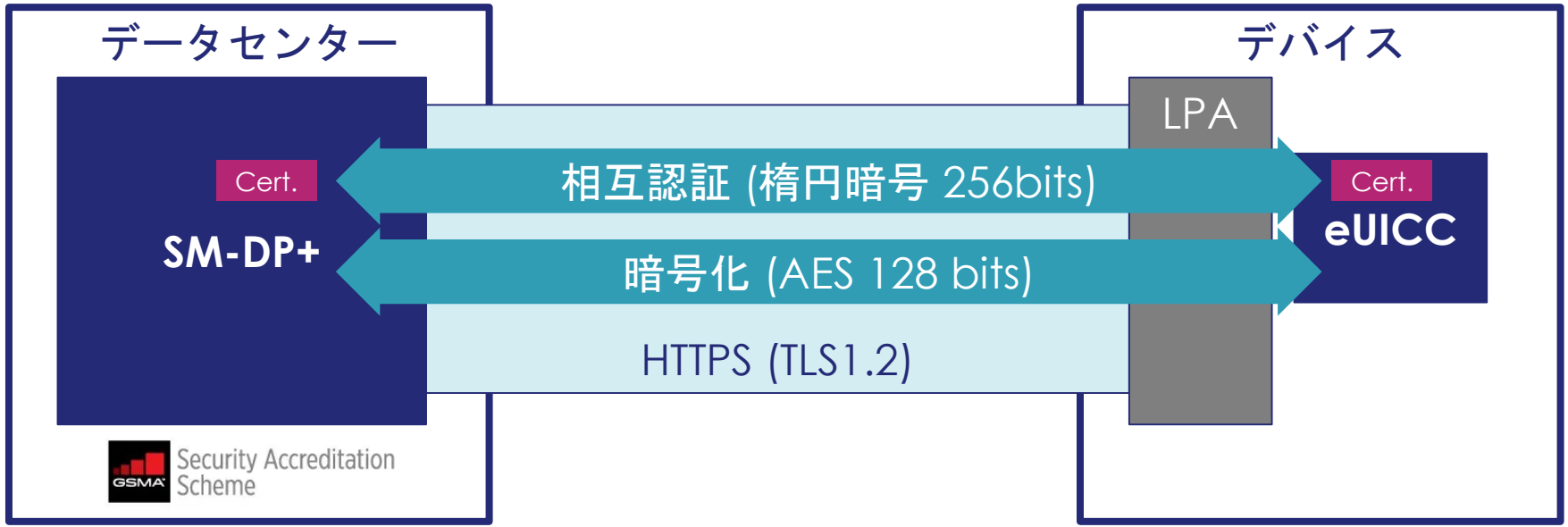
Supplier	Site	Scope of Certification					Valid to:	Cert.
		Secure Routing	Data Preparation	Data Preparation+ (ref. SGP.22)	Data Centre Operations & Management	Discovery Service		
Thales DIS France SA [1]	Tours, France	✓	✓	✓	✓	✓	Jan 2021	
Thales DIS (Shanghai) Co., Ltd. [1]	Shanghai, China	✓	✓	✓	✓	-	Sep 2021	
Thales DIS USA, Inc.	Dallas, USA	✓	✓	✓	✓	✓	Mar 2021	

OPEN

SM-DP+とeUICC間のセキュアな通信

LPAとSM-DP+の、通常のHTTPS(TLS1.2)通信に加え、

- eUICCとSM-DP+間のPKIによる相互認証、および
- eUICCとSM-DP+間のエンドツーエンドの暗号化を施して保護



GSMAによるPKIエコシステム

- GSMA CIにより発行され、相互認証に使用
  - EUM (eUICC Manufacturer)
  - SM-DP+
  - SM-DS (Discovery Service)
- GSMA SAS認定取得が必要
- PKI証明書ポリシー (SGP.14)
  - 証明書のライフサイクル管理や、CRLによる証明書の失効プロセスを定義

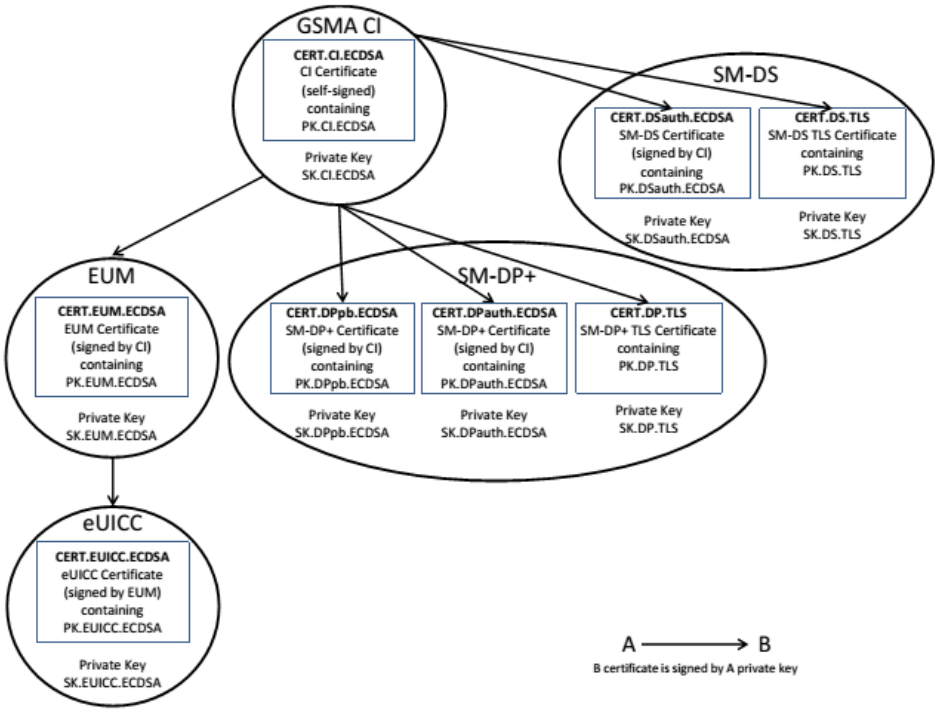


Figure 30: Certificate Chains

(Source: GSMA SGP.22)

CRL: Certificate Revocation List

GSMA仕様で言及されているその他のセキュリティメカニズム

エリジビリティチェック(オプション)

- オペレーターもしくはSM-DP+が、プロファイルダウンロード前に、eUICCやデバイスの情報を確認し、 プロファイルダウンロードに適しているかどうかを判断する

例

- EID (eUICC ID)
  - 現在は、ITU E.118に従い発行
  - eUICC Manufacture (EUM)の識別が可能
- eUICC Information
  - eUICCがサポートしている仕様書バージョンなどの各種情報
- Device Type Allocation Code (TAC)
  - IMEIの最初の8 digits
  - GSMAにより発行
  - デバイスの識別が可能

参考資料

GSMAコンプライアンスプロセス

- https://www.gsma.com/esim/compliance/

GSMAセキュリティアクレディテーションスキーム (SAS)

- https://www.gsma.com/security/security-accreditation-scheme/

GSMA SAS 認定取得拠点リスト

- https://www.gsma.com/security/sas-accredited-sites/

GSMA Intelligence

- eSIM moving up the agenda: from industry work to customer adoption (June 2020)
- https://data.gsmaintelligence.com/research/research/research-2020/esim-moving-up-the-agenda-from-industry-work-to-customer-adoption

Thales Digital Identity & Security

https://www.thalesgroup.com/en/dis-contact-us