

eSIMについて



株式会社インターネットイニシアティブ
大内 宗徳

Ongoing Innovation



はじめに

2018年3月からフルMVNOインフラを利用したサービスを開始しています。

このインフラを活用したサービスとして、eSIMを利用したサービス化の検討のため、2018年初夏から実証試験(PoC)を行いました。本セッションでは、PoCについてとeSIMの技術的な概要を共有します。

- スピーカー

- 大内 宗徳

- IIJ フルMVNO構想の初期段階から参画
 - フルMVNOのSIM/インフラの企画、設計/開発/検証を担当、国内/海外オペレータとの折衝
 - IIJmio meetingテクニカルセッションでの講演

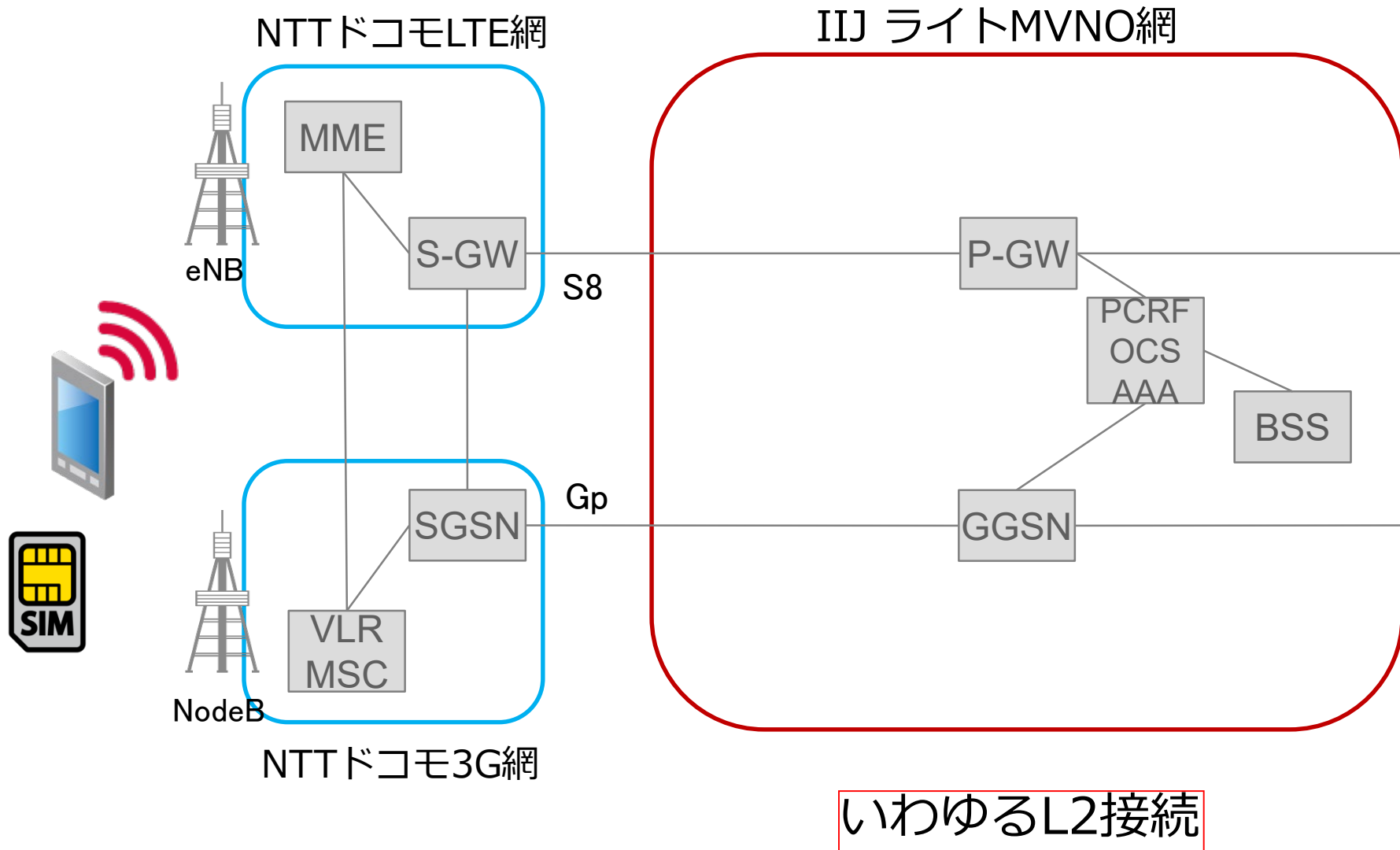
eSIM

- IIJ MVNOインフラ概要
- IIJ フルMVNOサービス領域
- eSIMとは？
- IIJ PoCについて
- eSIMの仕組みについて
- まとめ

eSIMについて

- IIJ MVNOインフラ概要
- IIJ フルMVNOサービス領域
- eSIMとは？
- IIJ PoCについて
- eSIMの仕組みについて
- まとめ

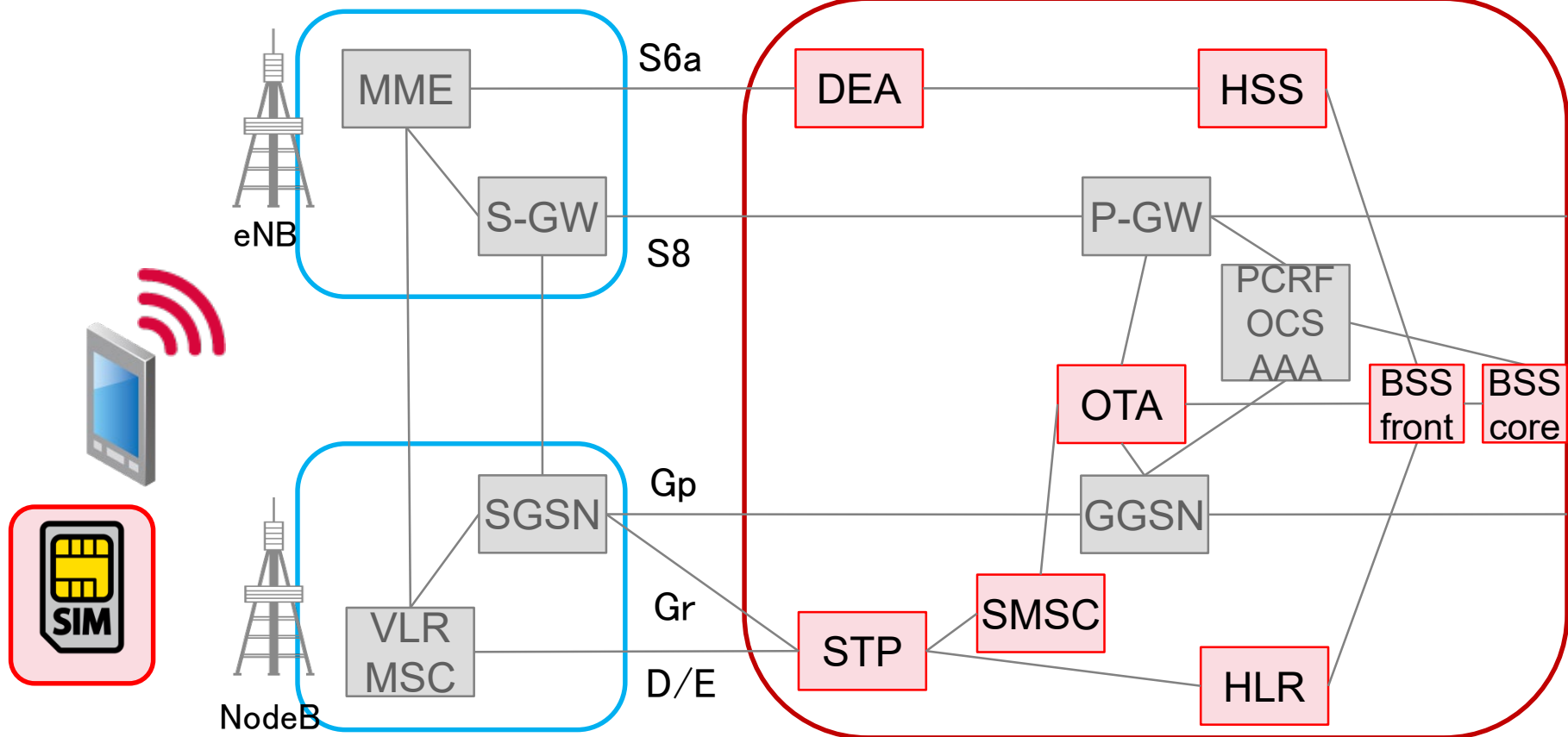
IIJ ライトMVNOインフラ概要



IIJ フルMVNOインフラ概要

NTTドコモLTE網

IIJ フルMVNO網



NTTドコモ3G網

加入者管理関連/OTA機能/IIJ独自SIMの開発

eSIMについて

- IIJ MVNOインフラ概要
- IIJ フルMVNOサービス領域
- eSIMとは？
- IIJ PoCについて
- eSIMの仕組みについて
- まとめ

IIJ フルMVNOサービス領域

個人向け
IoT/M2M
データ通信

訪日旅行者向け
データ通信

個人向け
海外データ通信

個人向け
データ通信

個人向け
音声通信

現在の主要なサービス領域

法人向け
海外データ通信

法人向け
データ通信

法人向け
音声通信

法人向け
IoT/M2M
データ通信

既存ライトMVNOのデータ通信部分の機能拡張やライトMVNOではサービス提供が柔軟にできない領域でのサービスを強化する！

フルMVNOを利用したサービス開発について

フルMVNOを利用して
サービスを拡充

個人向け
海外データ通信

法人向け
海外データ通信

国際ローミングオプション
(7月開始)

個人向け
IoT/M2M
データ通信

訪日旅行者向け
データ通信

個人向け
データ通信

法人向け
データ通信

法人向け
IoT/M2M
データ通信

IIJmio IoTサービス
(8月開始)

Japan Travel SIM
(4月開始)

個人向け
音声通信

個人向けデータ通信
現在の主要な
コンシューマ規格に
基づくeSIMサービス
(開発着手)

音声通信

ライフサイクル管理
(3月開始)

チップSIMの提供
(開発中)

eSIMについて

- IIJ MVNOインフラ概要
- IIJ フルMVNOサービス領域
- eSIMとは？
- IIJ PoCについて
- eSIMの仕組みについて
- まとめ

eSIMとは? - 1

GSMAが定義するコンシューマ仕様eSIMとは何か？
詳細は関連する規格書を読んでください！

GSMA SGP.21 - RSP Architecture
GSMA SGP.22 - RSP Technical Specification
GSMA SGP.23 - RSP Test Specification
GSMA SGP.24 - RSP Compliance Process
GSMA SGP.26 - RSP Test Certificates Definition

GSMA SGP.14 - GSMA eUICC PKI Certificate Policy
GSMA FS.04 - SAS-UP Standard
GSMA FS.05 - SAS-UP Methodology
GSMA FS.08 - SAS-SM Standard
GSMA FS.09 - SAS-SM Methodology
GSMA FS.17 - SAS Consolidated Security Requirements

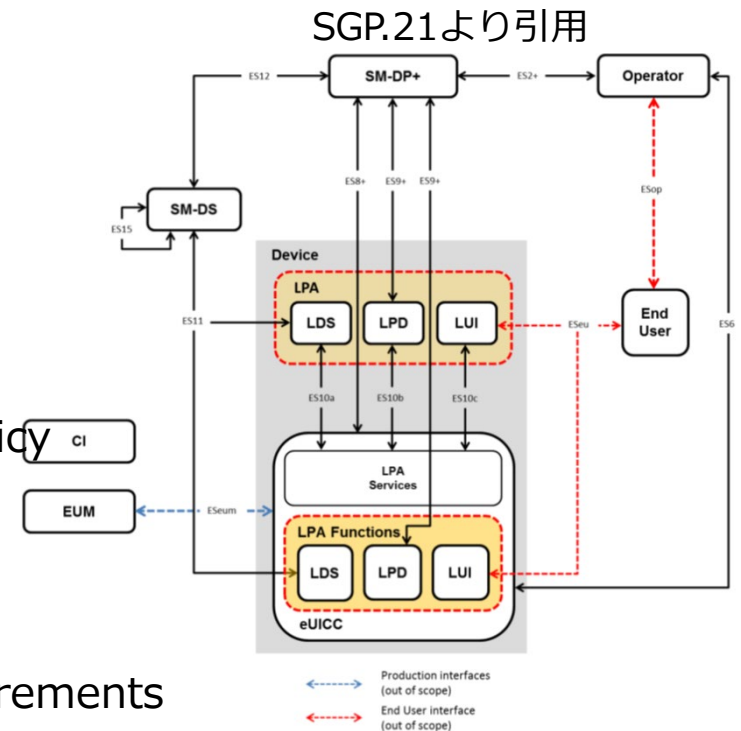


Figure 1: Remote SIM Provisioning System Architecture.

SIMalliance eUICC Profile Package: Interoperable Format Technical Specification

eSIMの説明は以上、終了！

eSIMとは? - 2

GSMAが定義するコンシューマ仕様eSIMとは何か？
詳細は関連する規格書を読んでください！

GSMA SGP.21 - RSP Architecture
GSMA SGP.22 - RSP Technical Specification
GSMA SGP.23 - RSP Test Specification
GSMA SGP.24 - RSP Certification

というわけには、当然いかないので、仕様書から読み取りにくい、eSIMを理解するために必要な基本的な概念等を含めた解説を次のページから。

GSMA FS.09 - SAS-SM Methodology
GSMA FS.17 - SAS Consolidated Security Requirements

SIMalliance eUICC Profile Package: Interoperable Format Technical Specification

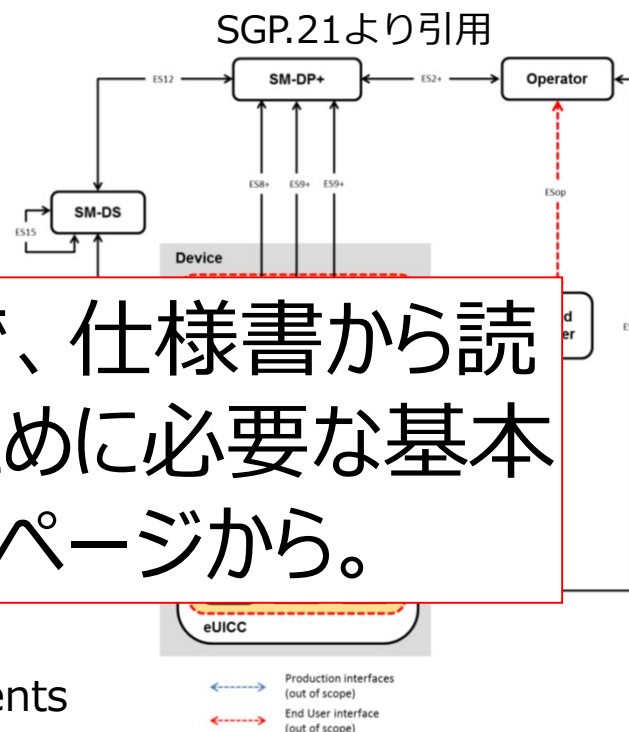
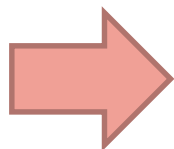


Figure 1: Remote SIM Provisioning System Architecture.

eSIMとは？ - 3

そもそも、SIM(Subscriber Identity Module)とは？



SIMカードは認証鍵情報を読み出させないようにセキュリティが強化されたマイコン

IMSI: **加入者識別子**(15桁の数字)
ユーザ名相当
(例) **44003**XXXXXXXXXX

Ki: **認証鍵**

パスワード相当

その他: 端末挙動を制御する値
独自のJavaプログラムも動作

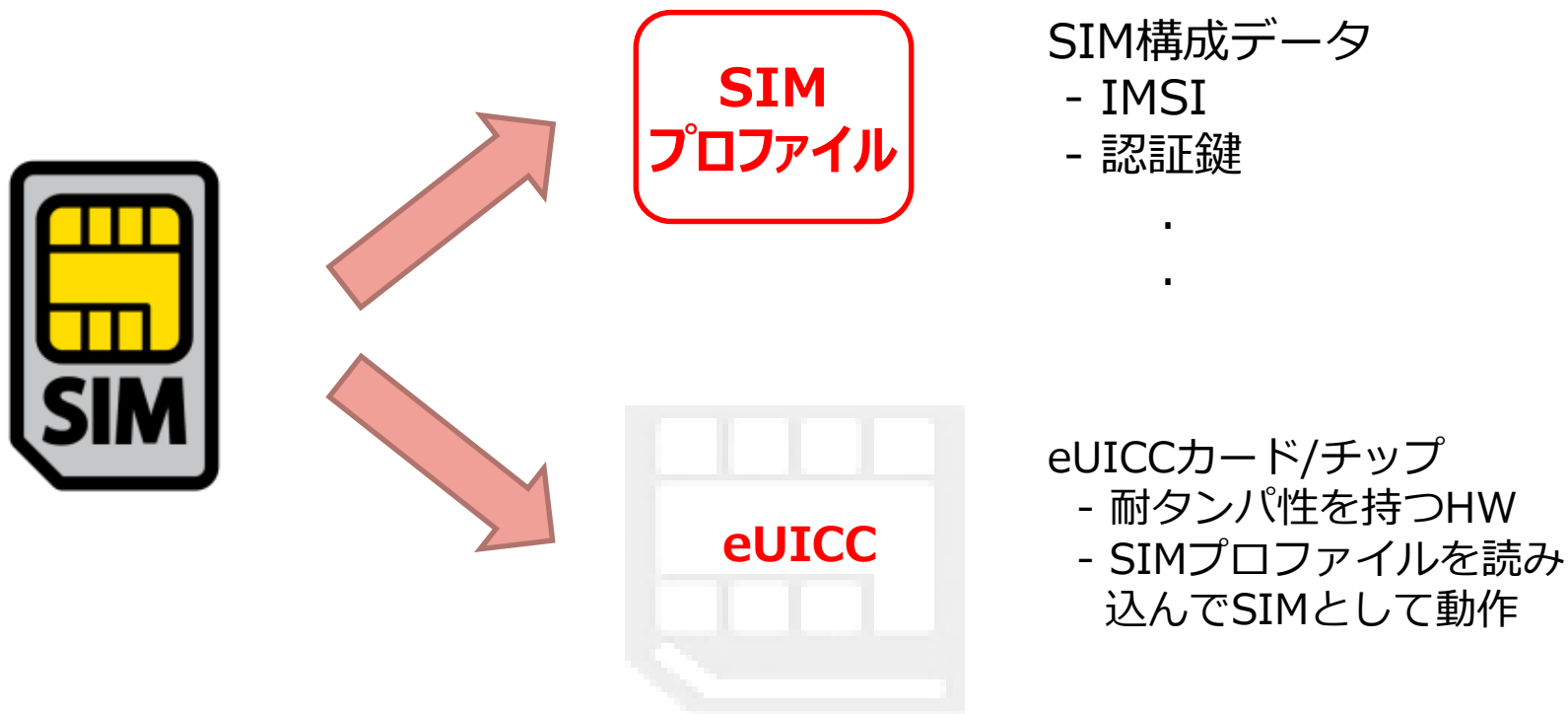
ハードの物理解析/読み出しを含めて耐タンパ性が強化されており、
認証鍵を抜き取ってのクローンSIM作成が非常に困難になっている

eSIMとは？ - 4

eSIM (embedded SIM) では、SIMカードの

- SIMデータの入れ物としてのハード
- SIMを構成するデータ

を分離して取り扱うのがポイント



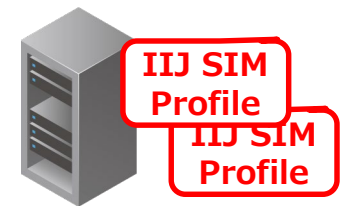
eSIMとは? - 5

SIMのハードとデータを分離することで今までとは異なる世界を実現できる

スマホ/タブレット

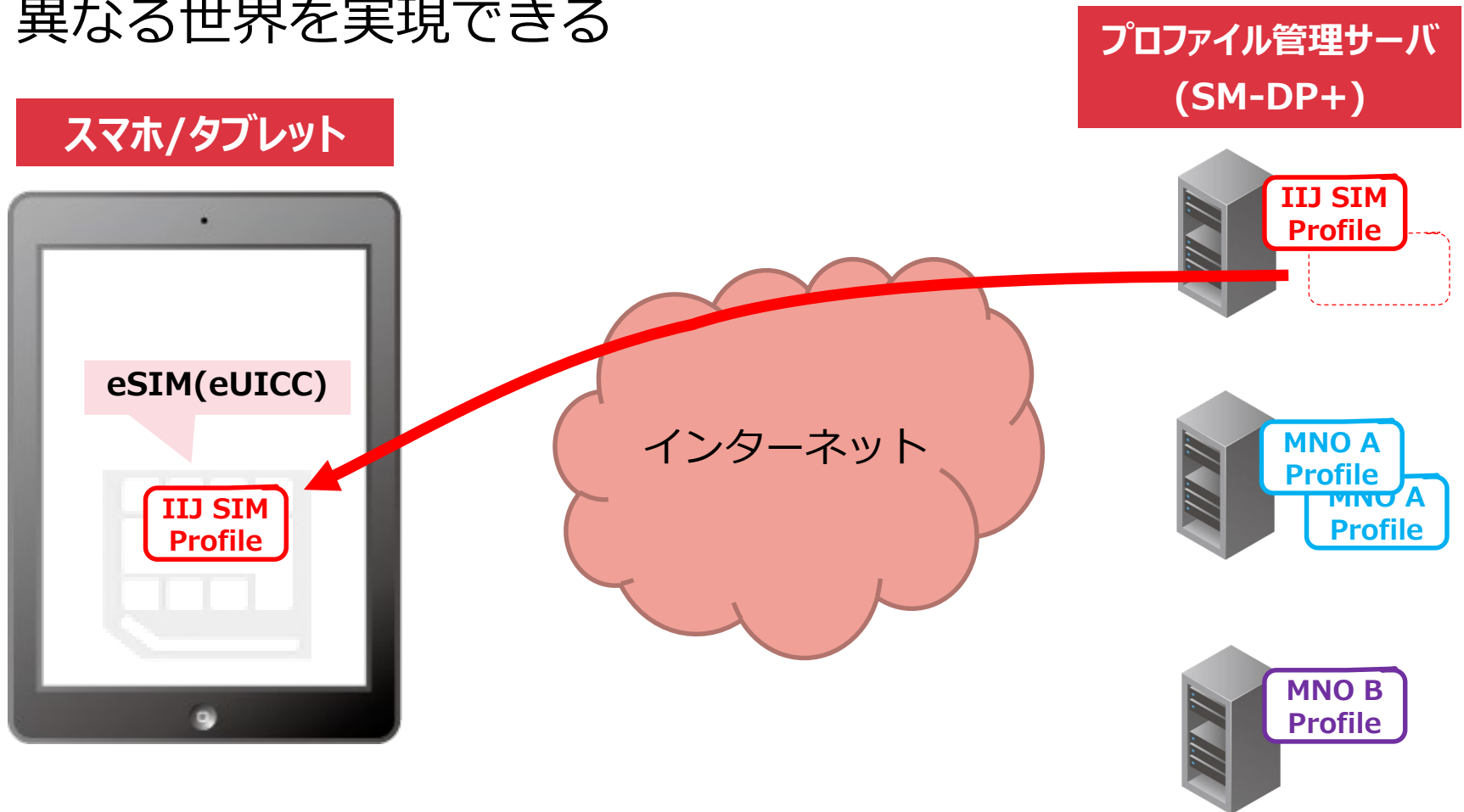


プロフィール管理サーバ
(SM-DP+)



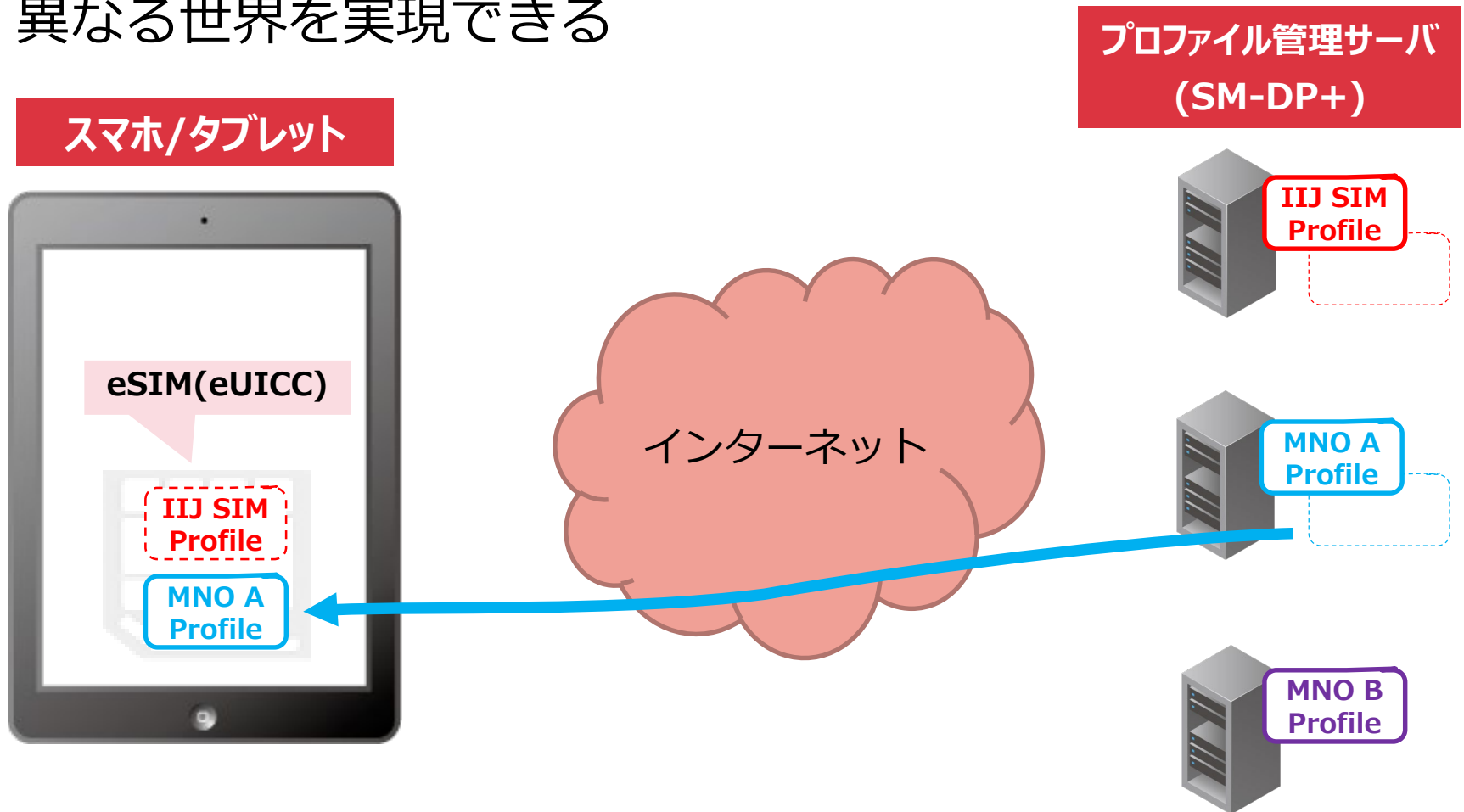
eSIMとは？ - 6

SIMのハードとデータを分離することで今までとは異なる世界を実現できる



eSIMとは? - 7

SIMのハードとデータを分離することで今までとは異なる世界を実現できる



eSIMとは？ - 8

SIMがデータ化されることで

- 交換時のSIMの物理的な抜き差しが不要
- 端末毎にSIMサイズを気にしなくて良い
- SIMがリアルタイムで利用可能
- SIM物理配送が不要
- SIMの物流在庫が不要
- SIMの盗難を気にする必要がない
- eSIMに複数のSIMプロフィール持てる
- 簡単に異なるキャリアに切替可能

メリットだらけだが、キャリアロックと相容れないMNOは↑の部分を非常に嫌がっている。

プロフィール管理サーバ

(SIM-DP+)

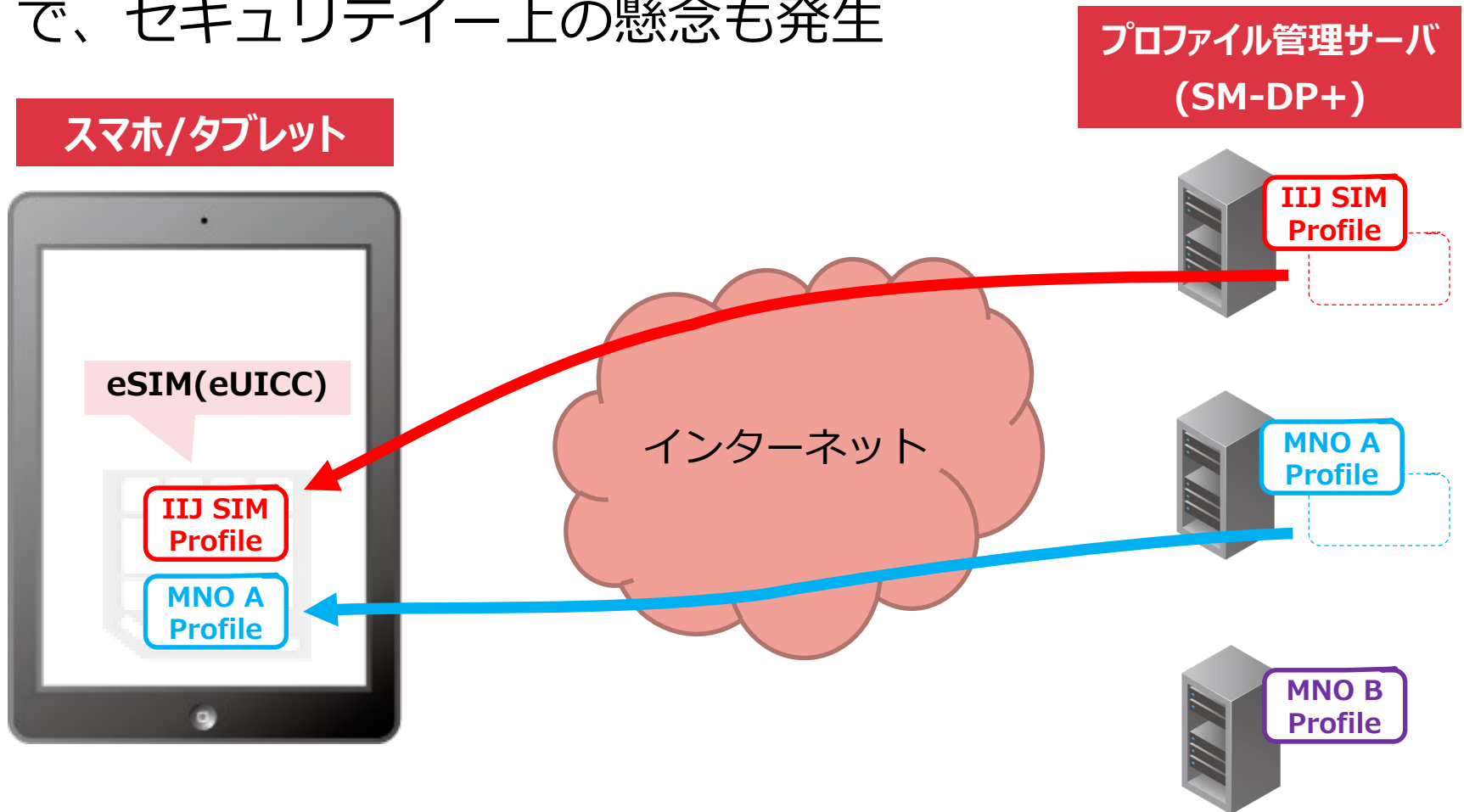
IIJ SIM Profile

MNO A Profile

MNO B Profile

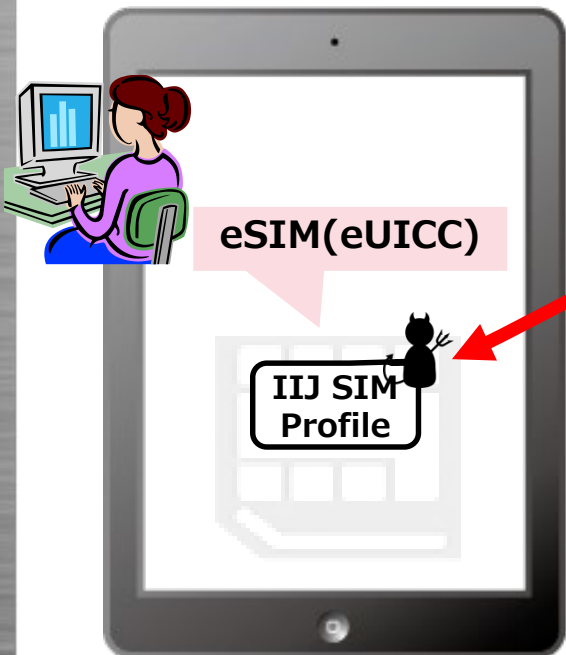
eSIMとは? - 9

SIMのデータ化やリモートサーバからDLを可能にしたことで、セキュリティー上の懸念も発生

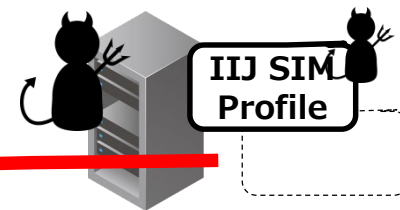


eSIMとは？ - 10

スマホ/タブレット



プロフィール管理サーバ
(SM-DP+)



不正なSM-DP+サーバから、不正なプロフィールをDLさせられていないか？

NO A profile

MNO B Profile

eSIMとは? - 11

スマホ/タブレット

eSIM(eUICC)

IIJ SIM Profile

eSIM(eUICC)

IIJ SIM Profile

サーバ上のSIMプロフィールを異なるeSIMにDLしてクローンSIMを作られたりしないか?

インターネット

プロフィール管理サーバ (SM-DP+)

IIJ SIM Profile

MNO A Profile

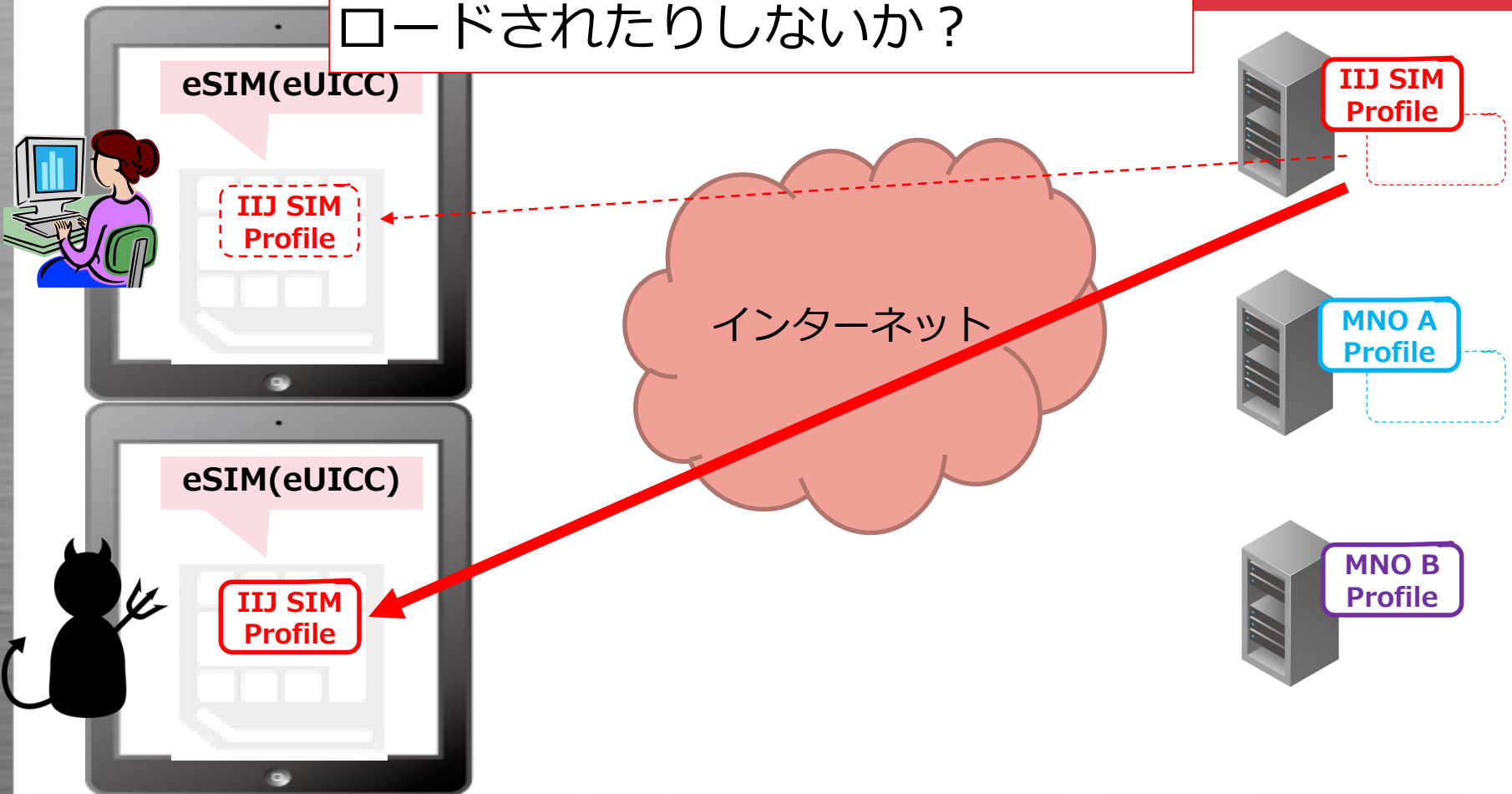
MNO B Profile



eSIMとは? - 12

スマホ/タブ SIMプロフィールを不正にダウンロードされたりしないか？

プロフィール管理サーバ (SM-DP+)

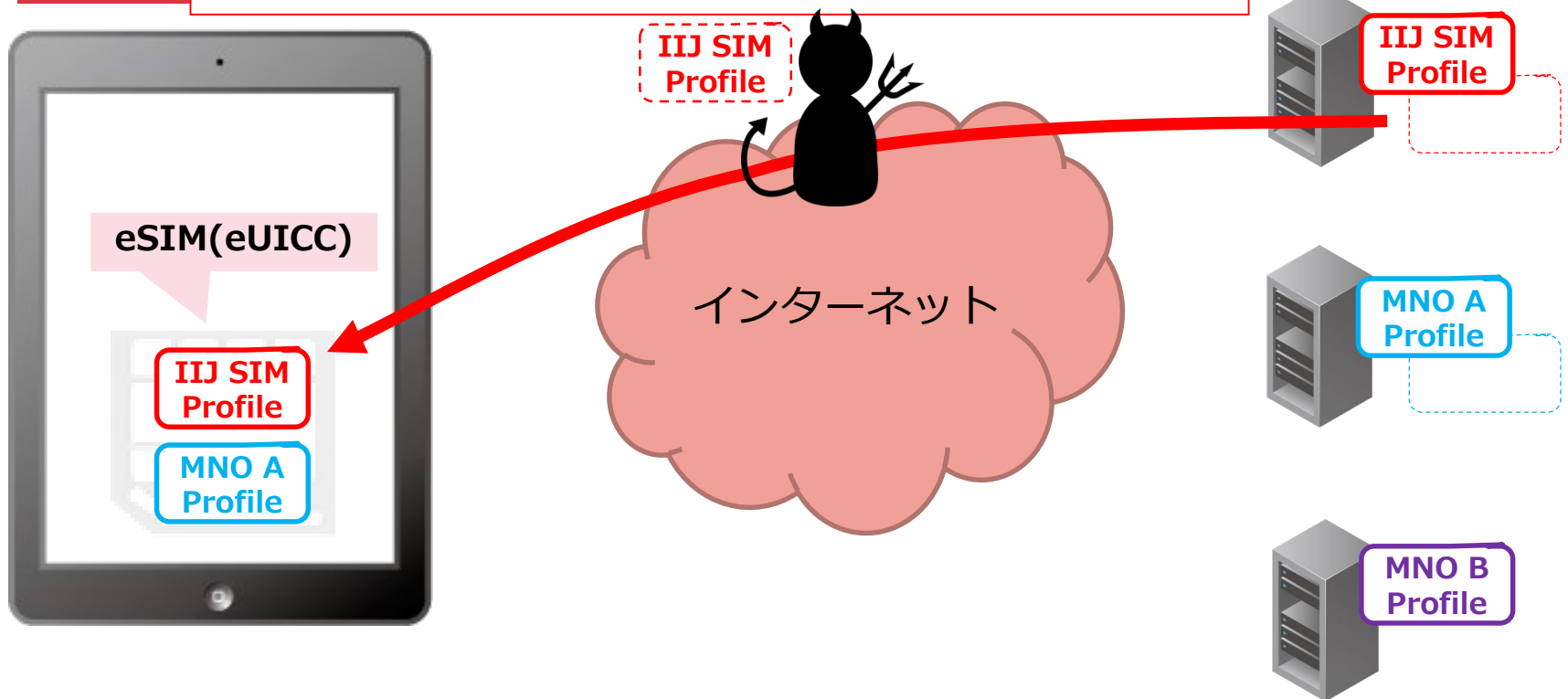


eSIMとは？ - 13

インターネット上でSIMプロファイル
を盗聴されて、クローンSIMを作られ
たりしないか？

スマホ

ファイル管理サーバ
(SM-DP+)

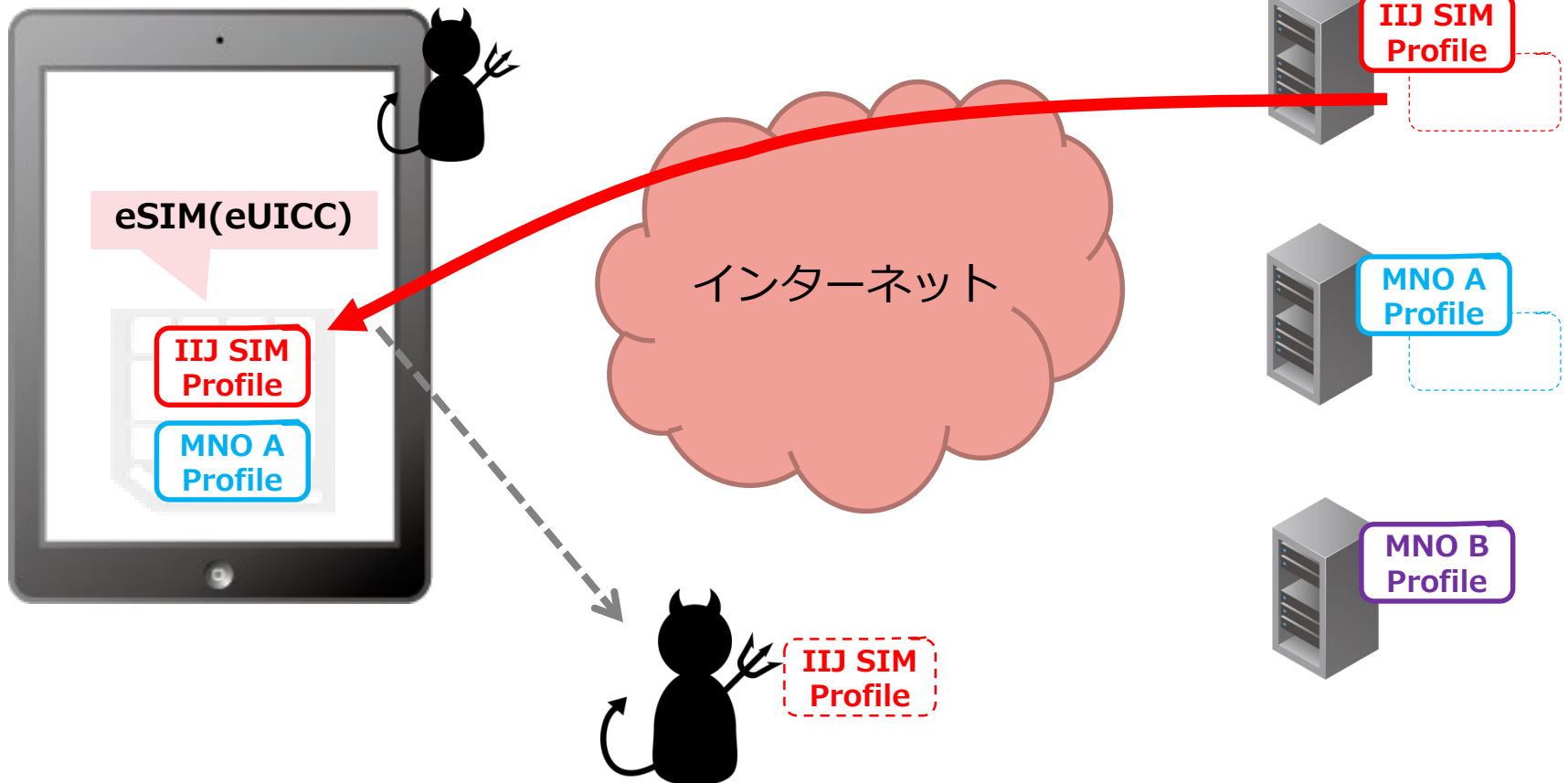


eSIMとは? - 14

不正な端末でSIMプロフィールを盗聴されたりしないか？

プロフィール管理サーバ
(SM-DP+)

スマホ/タブレット

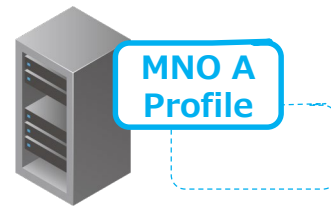
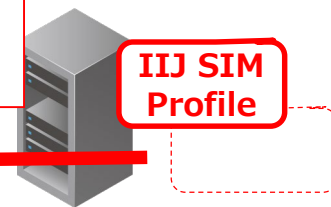
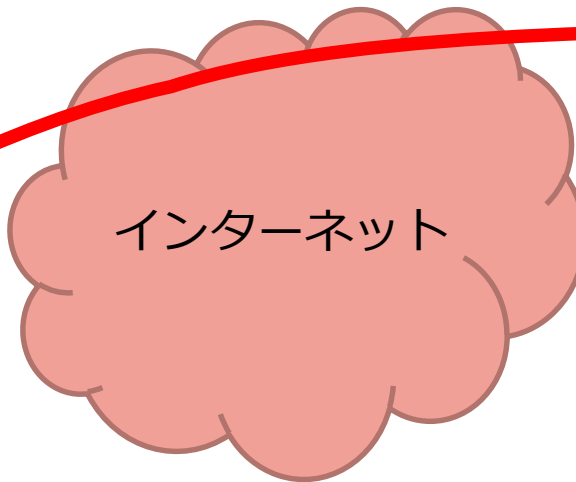
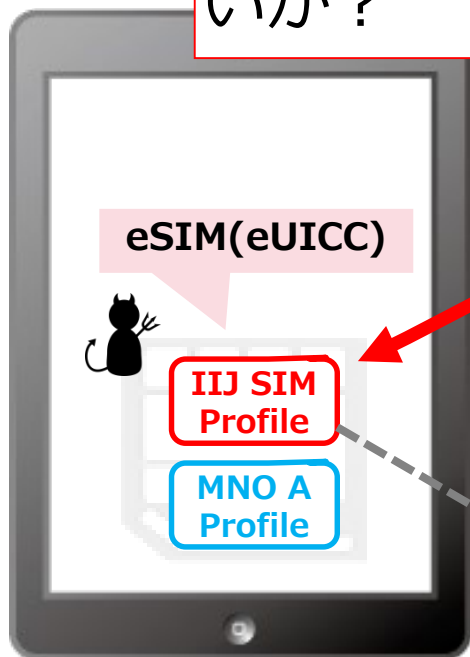


eSIMとは? - 15

スマホ

不正なeSIMでSIMプロファイルをコピーされて、クローンSIMを作られたりしないか？

ファイル管理サーバ (SM-DP+)



eSIMについて

- IIJ MVNOインフラ概要
- IIJ フルMVNOサービス領域
- eSIMとは？
- IIJ PoCについて
- eSIMの仕組みについて
- まとめ

IIJが実施したPoCについて - 1

- 2018年3月頃からPoCの準備着手し、初夏から試験開始
- IIJでGSMA Root CIから認証を受けたSM-DP+サーバとSIMプロファイルを用意
- PoC内容
 - IIJ SIMプロファイルをダウンロードして、商用網に接続可能かの確認
 - eSIM対応デバイスでの動作確認
 - Microsoft Surface Pro LTE Advanced
 - Windows PC(V社,H社)
 - Apple(iOS 12.1以降)
 - iPhone XS/XR, iPad Pro(2018年)
 - eSIM内蔵Android端末(デバイス名非公開)
 - 主要SIMサプライヤーからeSIMカードを調達し動作確認

IIJが実施したPoCについて - 2

- Microsoft Surface Pro LTE Advanced
IIJ、フルMVNOとしてeSIM搭載端末の動作検証を開始(2018/7/12)
<https://www.ij.ad.jp/news/pressrelease/2018/0712.html>

The screenshot displays the Windows 10 'eSIM Profile Management' settings. A new eSIM profile is being added, with the following details highlighted in a blue box:

- Carrier: IIJ
- ICCID: 8981030390000000176F
- Profile Name: 8981030390000000176

The interface shows the 'eSIM Profile Management' screen with a list of profiles. The newly added profile is shown as 'IIJ 8981030390000000176F' and is marked as 'アクティブ' (Active). The status bar at the bottom right shows the active network as 'IIJ (LTE) 接続済み' (Connected).

IIJが実施したPoCについて - 3

- iPhone XS (物理SIM+eSIMにIIJプロファイル) (2018/10/30)



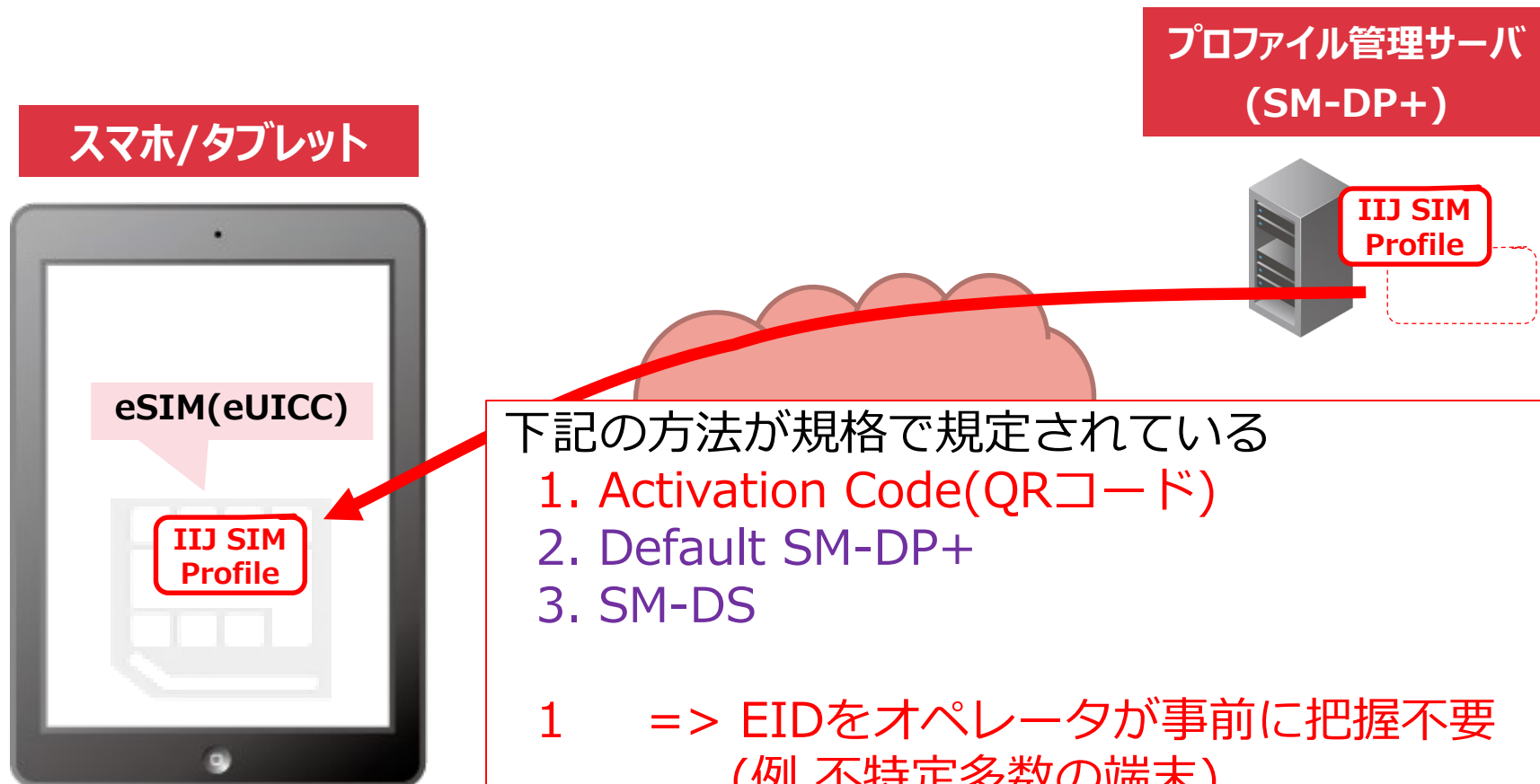
eSIMについて

- IIJ MVNOインフラ概要
- IIJ フルMVNOサービス領域
- eSIMとは？
- IIJ PoCについて
- eSIMの仕組みについて
 - プロファイルのDL
 - SIMプロファイルとは
 - eUICCとは
 - eSIMのセキュリティの仕組み
 - LPAとは
- まとめ

eSIMについて

- IIJ MVNOインフラ概要
- IIJ フルMVNOサービス領域
- eSIMとは？
- IIJ PoCについて
- eSIMの仕組みについて
 - プロファイルのDL
 - SIMプロファイルとは
 - eUICCとは
 - eSIMのセキュリティの仕組み
 - LPAとは
- まとめ

プロファイルのダウンロード方法 - 1



下記の方法が規格で規定されている

1. Activation Code(QRコード)
2. Default SM-DP+
3. SM-DS

1 => EIDをオペレータが事前に把握不要
(例 不特定多数の端末)

2, 3 => EIDをオペレータで事前把握の必要有
(例 オペレータが販売している端末)

EID: eSIM(eUICC)の個体識別子

プロファイルのダウンロード方法 - 2

Activation Codeとは？

Examples of the Activation Code are as follows:

SM-DP+アドレス

Matching ID

(サーバ上のプロファイルを一意に指定)

- 1\$SMDP.GSMA.COM\$04386-AGYFT-A74Y8-3F815
(if SM-DP+ OID and Confirmation Code Required Flag are not present)
- 1\$SMDP.GSMA.COM\$04386-AGYFT-A74Y8-3F815\$\$1 Confirmationコードを必要とするか
(if SM-DP+ OID is not present and Confirmation Code Required Flag is present)
- 1\$SMDP.GSMA.COM\$04386-AGYFT-A74Y8-3F815\$1.3.6.1.4.1.31746\$1
(if SM-DP+ OID and Confirmation Code Required flag are present)
- 1\$SMDP.GSMA.COM\$04386-AGYFT-A74Y8-3F815\$1.3.6.1.4.1.31746
(If SM-DP+ OID is present and Confirmation Code Required Flag is not present)
- 1\$SMDP.GSMA.COM\$\$1.3.6.1.4.1.31746 サーバの認証用証明書(Cert.DPauth.DCDSA)のOID
(If SM-DP+ OID is present, Activation token is left blank and Confirmation Code Required Flag is not present)

When entered manually, the Activation Code SHALL be used as defined above.

When provided in a QR code according to ISO/IEC 18004 [15], the Activation Code SHALL be prefixed with "LPA:"



SGP.22 4.1 Activation Code から引用

QRコードは、LPA:1\$SMDP.GSMA.COM\$… のようになる

プロファイルのダウンロード方法 - 3

• SGP.21(eSIM)の世界

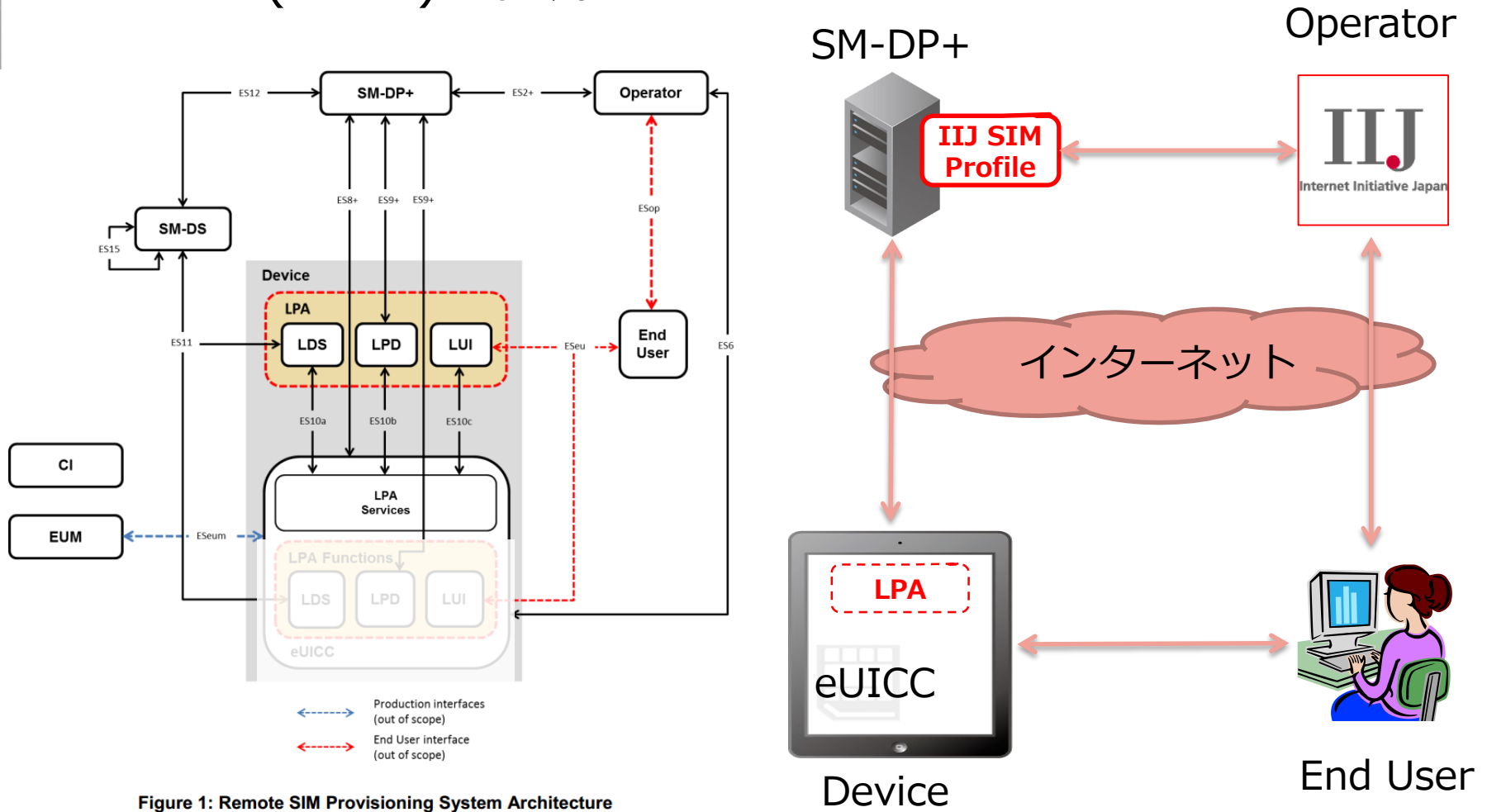


Figure 1: Remote SIM Provisioning System Architecture

SGP.21より引用

プロファイルのダウンロード方法 - 4

1. Activation Code(QRコード)

7. Matching ID
確認 -> OK

3. プロファイル/
Matching ID割当

2. 契約OK
各種プロビ
ジョニング
実施

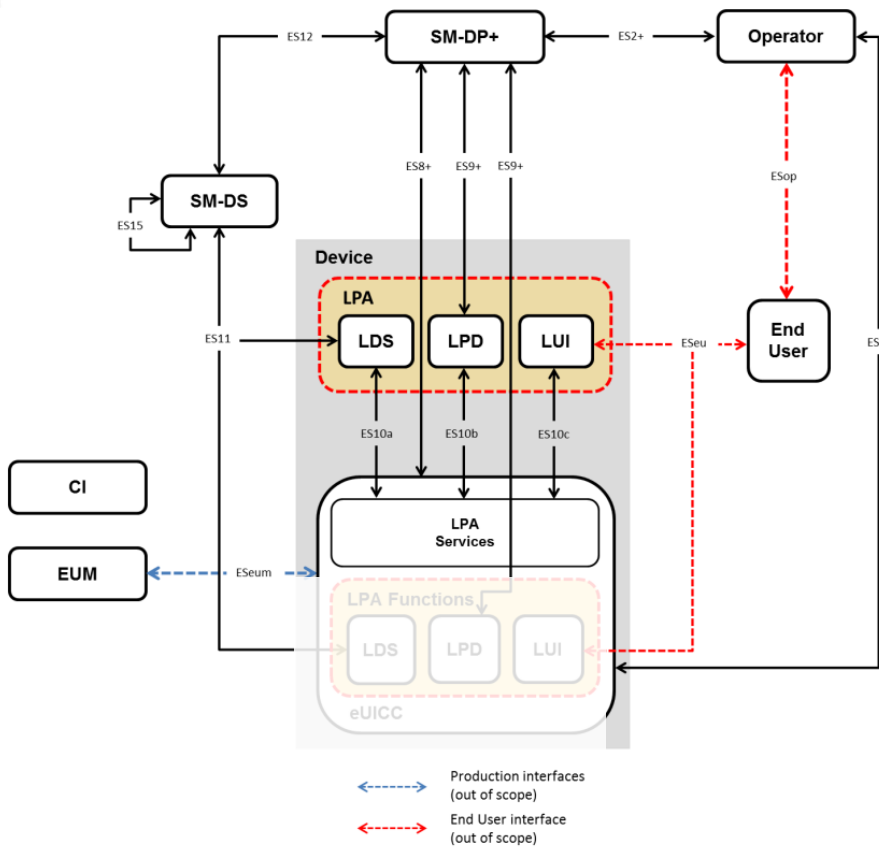
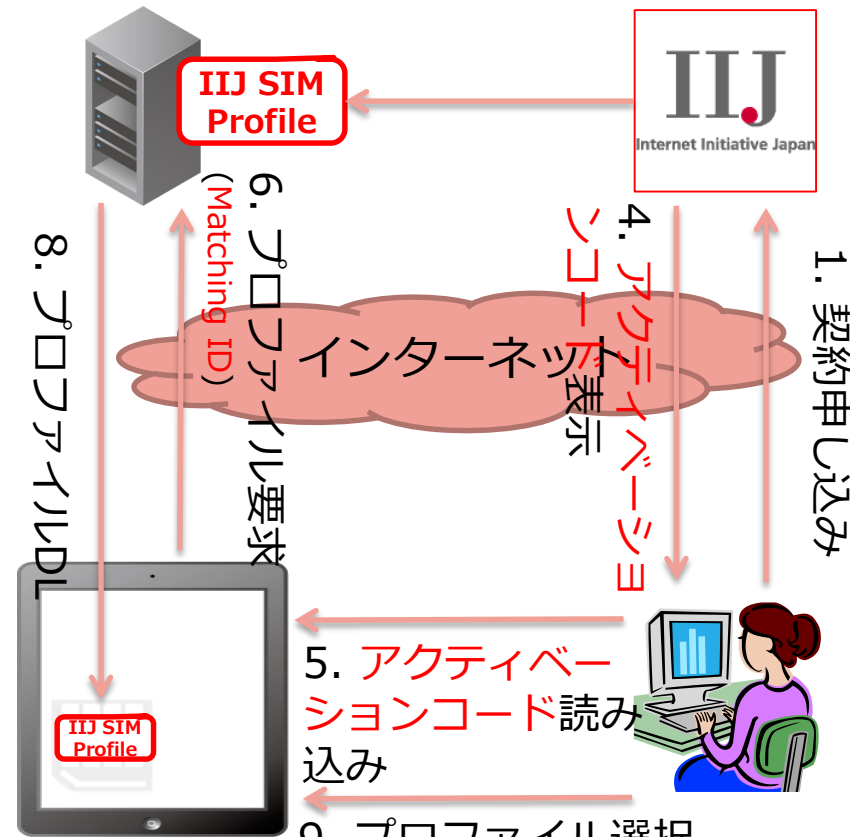


Figure 1: Remote SIM Provisioning System Architecture

SGP.21より引用



5. アクティベ
ションコード読み
込み

9. プロファイル選択
利用開始!

プロファイルのダウンロード方法 - 5

1. Activation Code (QRコード未使用の場合)

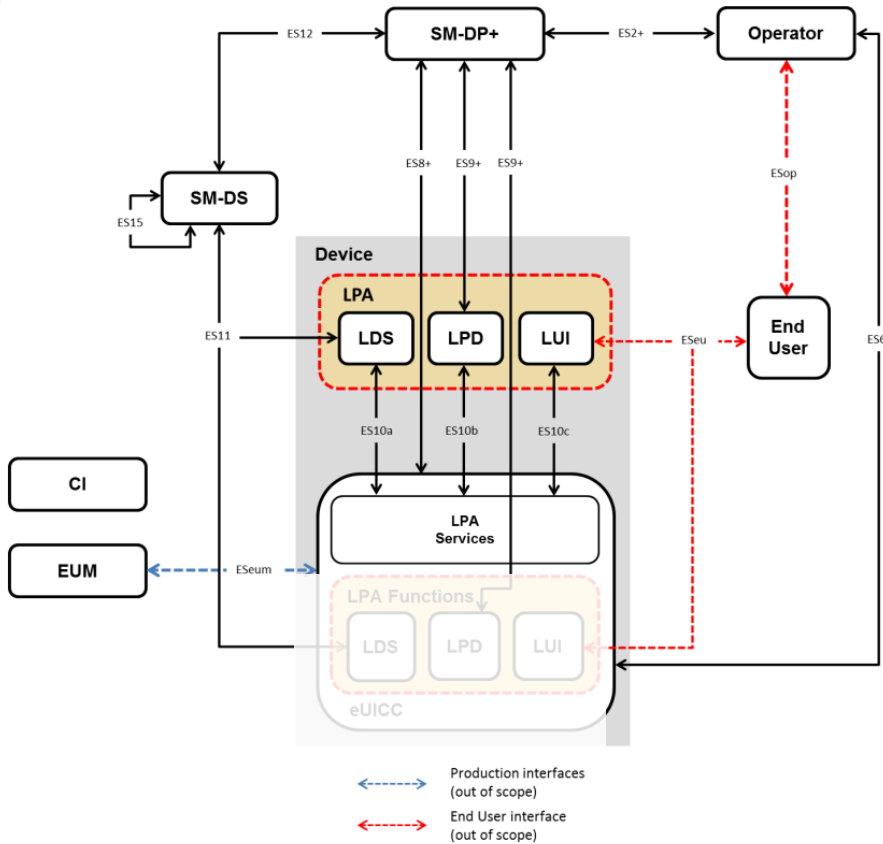


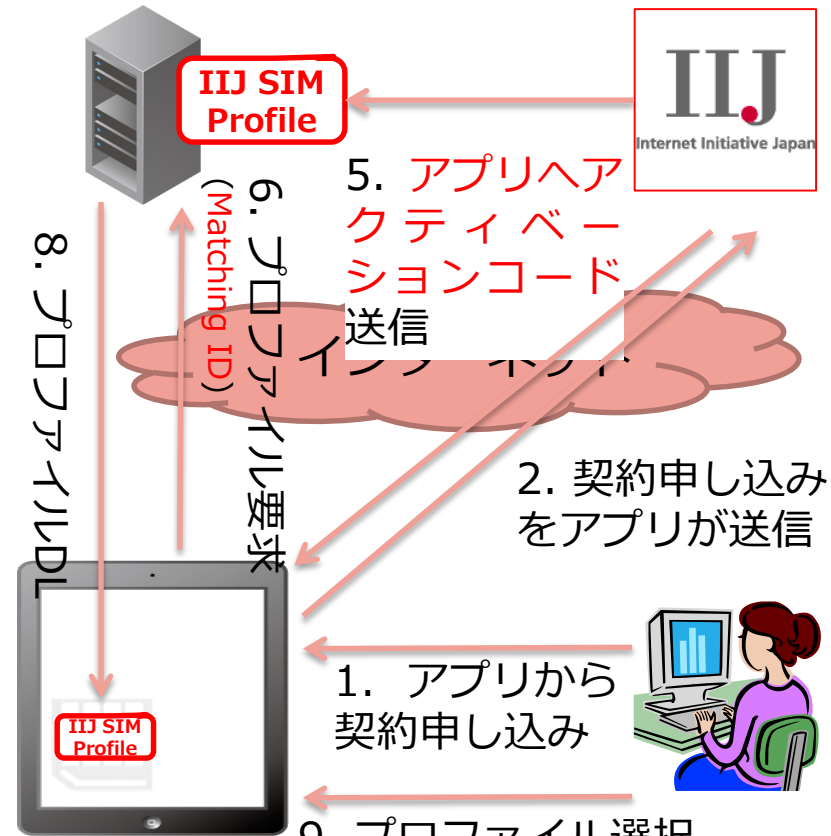
Figure 1: Remote SIM Provisioning System Architecture

SGP.21より引用

7. Matching ID 確認 -> OK

4. プロファイル/
Matching ID 割当

3. 契約OK
各種プロビ
ジョニング
実施



1. アプリから
契約申し込み

2. 契約申し込み
をアプリが送信

9. プロファイル選択
利用開始!

プロファイルのダウンロード方法 - 6

2. Default SM-DP+

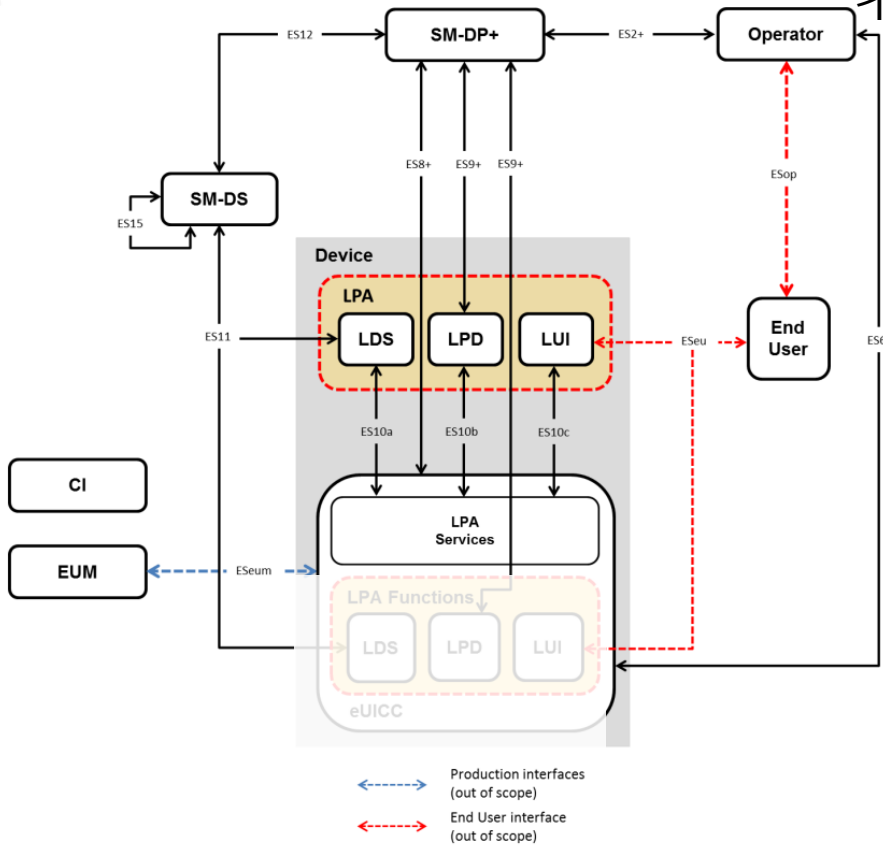
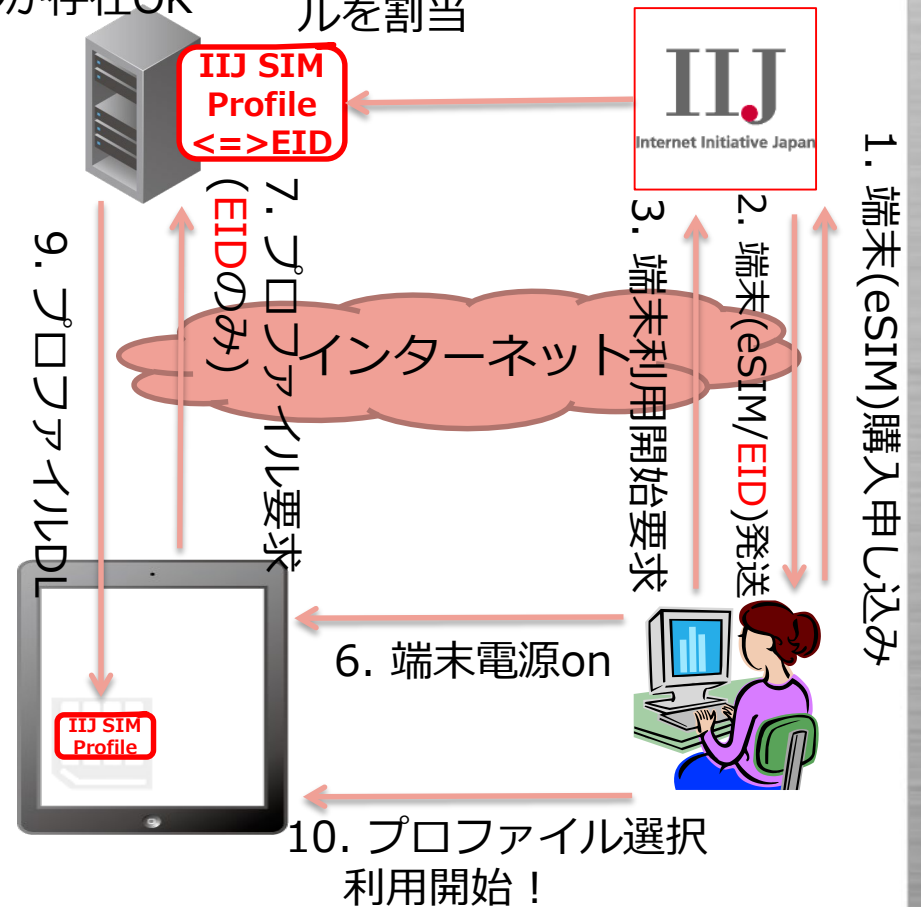


Figure 1: Remote SIM Provisioning System Architecture

SGP.21より引用

4. 各種プロビジョニング実施
5. eSIM(EID)に紐づくプロファイルを割り当
8. 端末eSIM(EID)に紐づくプロファイルが存在OK



プロファイルのダウンロード方法 - 7

3. SM-DS

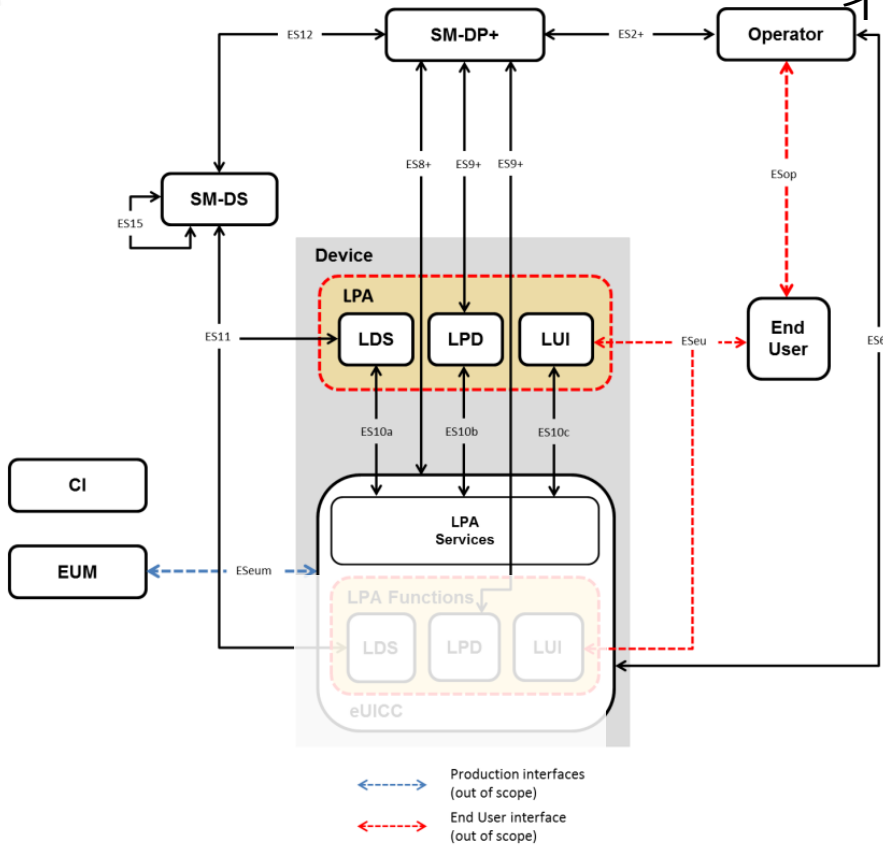
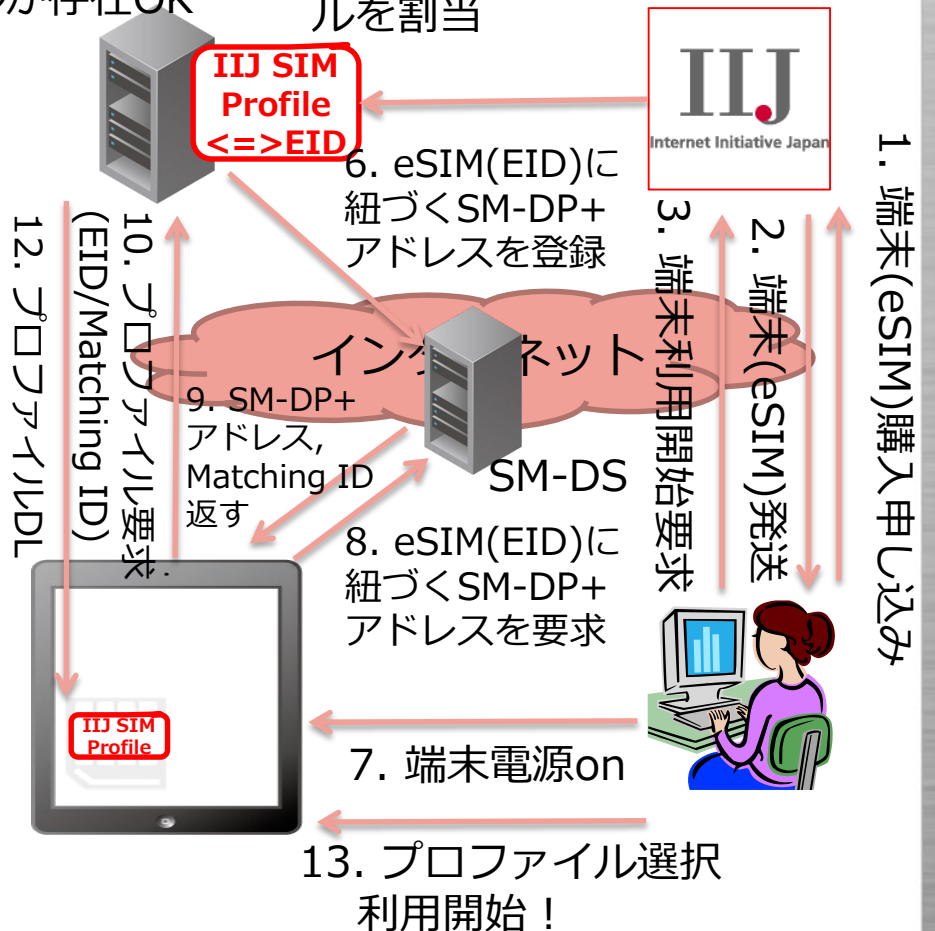


Figure 1: Remote SIM Provisioning System Architecture

SGP.21より引用

- 11. 端末eSIM(EID)に紐づくプロファイルが存在OK
- 5. eSIM(EID)に紐づくプロファイルを割り当
- 4. 各種プロビジョニング実施



eSIMについて

- IIJ MVNOインフラ概要
- IIJ フルMVNOサービス領域
- eSIMとは？
- IIJ PoCについて
- eSIMの仕組みについて
 - プロファイルのDL
 - SIMプロファイルとは
 - eUICCとは
 - eSIMのセキュリティの仕組み
 - LPAとは
- まとめ

SIMプロフィールとは - 1

- eUICC HW実装に依存せず、SIMが持つ機能、ファイル/認証/セキュリティ等を記述したデータフォーマット
 - GSMAでなく、SIMalliance(SIMベンダーの業界団体)の規格で定義
- プロファイルについて
 - eUICCチップ(カード)とSM-DP+サーバ間の直接暗号化でやり取りされるため、途中でSIM認証情報などの重要な情報の盗聴は非常に困難
 - プロファイルデータは役割(機能)単位で、Profile Elementというブロック単位で記述
 - DER(ASN.1)でデータを記述
 - eUICCはこのデータをサーバから読み込んで内部でSIM情報として展開
 - テンプレート機能があり、一部の値は指定しなくても、規格上で定義されているデフォルト値で補完してもらえ
 - ただし、この機能を使うと異なるeUICCベンダーで正常に動作しない場合がある

SIMプロフィールとは - 2

- SIMプロフィールの具体例について – Profile Element

Profile Element	Comments
ProfileHeader	
PE-MF	ICCID等を含むディレクトリの記述
PE-PUKCodes	Only one set of PUK codes exist in a Profile Package
PE-PINCodes	Creates the Global PIN codes
PE-TELECOM	
PE-GenericFileManagement	To be repeated in order to create the files required in the DF Phonebook under DF Telecom
PE-USIM	Creates a USIM ADF and the associated files
PE-OPT-USIM	IMSIなどを含むディレクトリの記述
PE-PHONEBOOK	Creates DF PHONEBOOK under USIM ADF
PE-AKAParameter	Sets the AKA parameters related to the previously created USIM
PE-PINCodes	Creates the local PIN code structure at the USIM ADF level
PE-GenericFileManagement	To be repeated in order to create additional files required in the ADF USIM
PE-GSM-ACCESS	
PE-SecurityDomain	Creates the MNO-SD
PE-SecurityDomain	Creates a SSD
PE-Application	Loads a USAT application
PE-Application	Loads an application in the SSD
PE-RFM	Sets the RFM parameters for the Profile
PE-End	End of the Profile Package

SIM認証の
鍵情報の記述

OTA認証の記述

OTAの設定関連

SIMalliance, eUICC Profile Package: Interoperable Format Technical Specification Ver. 2.2 -> 11.1 Example of Profile Package structure から引用

SIMプロフィールとは - 3

- SIMプロフィールの具体例について – Profile HEADER

11.2.2 Profile HEADER

ASN.1 Format	DER TLV encoding
<pre>headerValue ProfileElement ::= header : { major-version 2, minor-version 2, profileType "SIMalliance Sample Profile", iccid '89019990001234567893'H, eUICC-Mandatory-services { usim NULL, milenage NULL, javacard NULL }, eUICC-Mandatory-GFSTEList { { 2 23 143 1 2 1 }, --id-MF { 2 23 143 1 2 4 } --id-USIM } }</pre>	<pre>A0 48 80 01 02 81 01 02 82 1A 53494D616C6C69616E63652053616D706C652050726F66696C65 83 0A 89019990001234567893 A5 06 81 00 84 00 8B 00 A6 10 06 06 67810F010201 06 06 67810F010204</pre>

SIMalliance, eUICC Profile Package: Interoperable Format Technical Specification
Ver. 2.2 から引用

SIMプロファイルとは - 4

- SIMプロファイルの具体例について – PE MF

11.2.3 PE MF (Using Template)

ASN.1 Format	DER TLV encoding
<pre> mfVal ProfileElement ::= mf : { mf-header { mandated NULL, identification 1 }, templateID { 2 23 143 1 2 1 }, mf { fileDescriptor : { pinStatusTemplateDO '01020A'H } }, ef-pl { fileDescriptor : { -- EF PL modified to use Access Rule 15 within EF ARR securityAttributesReferenced '0F'H } }, ef-iccid { -- swapped ICCID: 98109909002143658739 fillFileContent : '98109909002143658739'H }, ef-dir { fileDescriptor : { </pre>	<pre> B0 8201F8 A0 05 80 00 81 01 01 81 06 67810F010201 A2 07 A1 05 C6 03 01020A A3 05 A1 03 8B 01 0F A4 0C 83 0A 98109909002143658739 A5 27 A1 09 </pre>

SIMalliance, eUICC Profile Package: Interoperable Format Technical Specification
Ver. 2.2から引用

SIMプロファイルとは - 5

- SIMプロファイルの具体例について – PE USIM

11.2.7 PE USIM (Using Template)

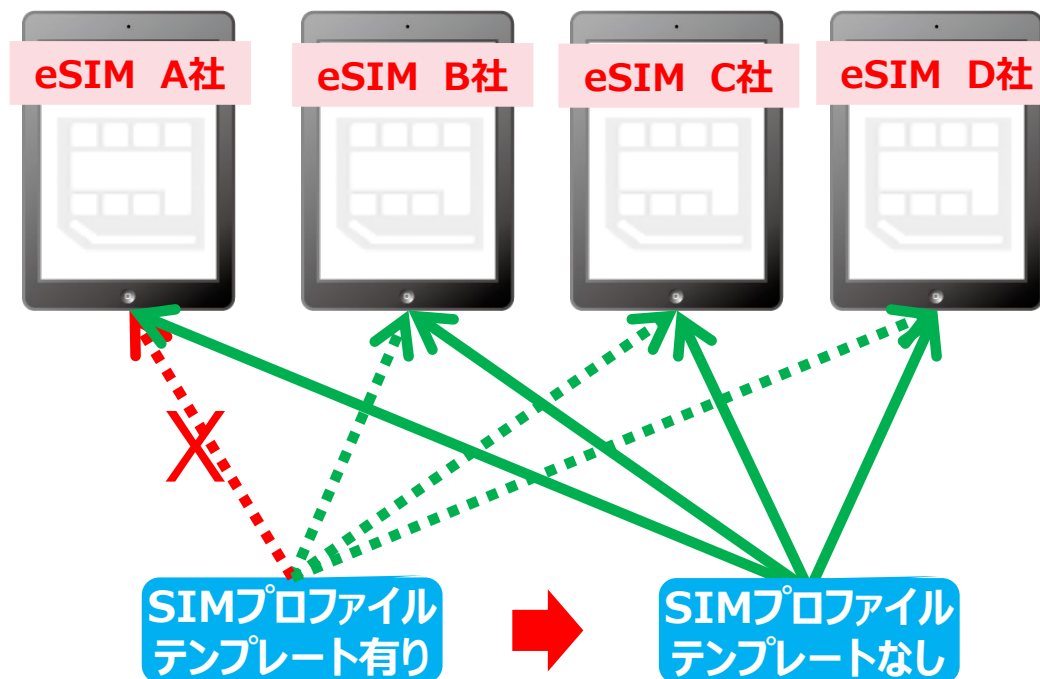
ASN.1 Format	DER TLV encoding
<pre>usimValue ProfileElement ::= usim : { usim-header { mandated NULL, identification 4 }, templateID { 2 23 143 1 2 4 }, adf-usim { fileDescriptor : { fileID '7FF1'H, dfName 'A0000000871002FF33FF018900000100'H, pinStatusTemplateDO '01810A'H } }, </pre>	<pre>B3 77 A0 05 80 00 81 01 04 81 06 67810F010204 A2 1D A1 1B 83 02 7FF1 84 10 A0000000871002FF33FF018900000100 C6 03 01810A</pre>
<pre>ef-imsi { -- numerical format: 234101943787656 fillFileContent : '082943019134876765'H }, ef-arr { fileDescriptor : { linkPath '2F06'H } }, ef-ust { -- Service Dialling Numbers, Short Message Storage fillFileContent : '0A2E178CE73204000000000000'H }, ef-spn { -- ASCII format: "SIMalliance" fillFileContent : '0253494D616C6C69616E6365'H }, </pre>	<pre>A3 0B 83 09 082943019134876765 A4 06 A1 04 C7 02 2F06 A8 0F 83 0D 0A2E178CE73204000000000000 AD 0E 83 0C 0253494D616C6C69616E6365</pre>

SIMalliance, eUICC Profile Package: Interoperable Format Technical Specification Ver. 2.2から引用

SIMプロフィールとは - 6

- 実証試験で遭遇した問題

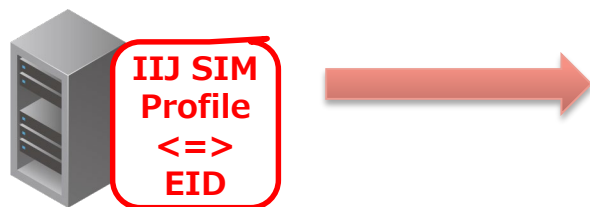
- eSIMベンダーが異なる場合に、プロフィールDLが失敗するケースがあった
- 標準化されているがプロフィールデータ解釈の互換性の問題があった
- 商用展開前には、SIMプロフィールが各社のeSIMで動作するか十分な検証が必要



SIMプロフィールとは - 7

サーバ上の各プロフィールは状態を持って管理されている

プロフィール管理サーバ
(SM-DP+)



重複ダウンロードを防ぐために、各プロフィールは状態を持ち、また、EIDに紐付けて管理される

3.1.6 Profile Lifecycle at SM-DP+

The previous sections provide detailed procedures associated with Remote Provisioning. Each Profile has state information on the SM-DP+ associated with it during the provisioning into an eUICC. The Profile lifecycle state can be one of the states listed in the following table.

Additional states and additional or customised ES2+ functions MAY be agreed between the Operator and the SM-DP+.

State Name	Description
Available	The Profile is available in the inventory of the SM-DP+.
Allocated	The Profile is reserved for downloading without being linked to an EID.
Linked	The Profile is reserved for downloading and is linked to an EID.
Confirmed	The Profile is reserved for downloading (linked or not linked to an EID) with Matching ID and Confirmation Code if required.
Released	The Profile is ready for download and installation after Network Configuration by the Operator (e.g.: HLR Registration).
Downloaded	The Bound Profile was delivered to the LPA.
Installed	The Profile was successfully installed on the eUICC.
Error	The Profile has not been installed because of one of the following error cases: <ul style="list-style-type: none"> - Confirmation Code Retry Limit exceeded - Download Retry Limit exceeded - End User Rejection - Error during download and installation
Unavailable	The Profile cannot be reused anymore by the SM-DP+.

Table 6b: Profile State in the SM-DP+

SGP.22より引用

SIMプロフィールとは - 8

サーバ上の各プロフィールは、サーバ仕様にもよるが、基本的には暗号化された状態で保管される

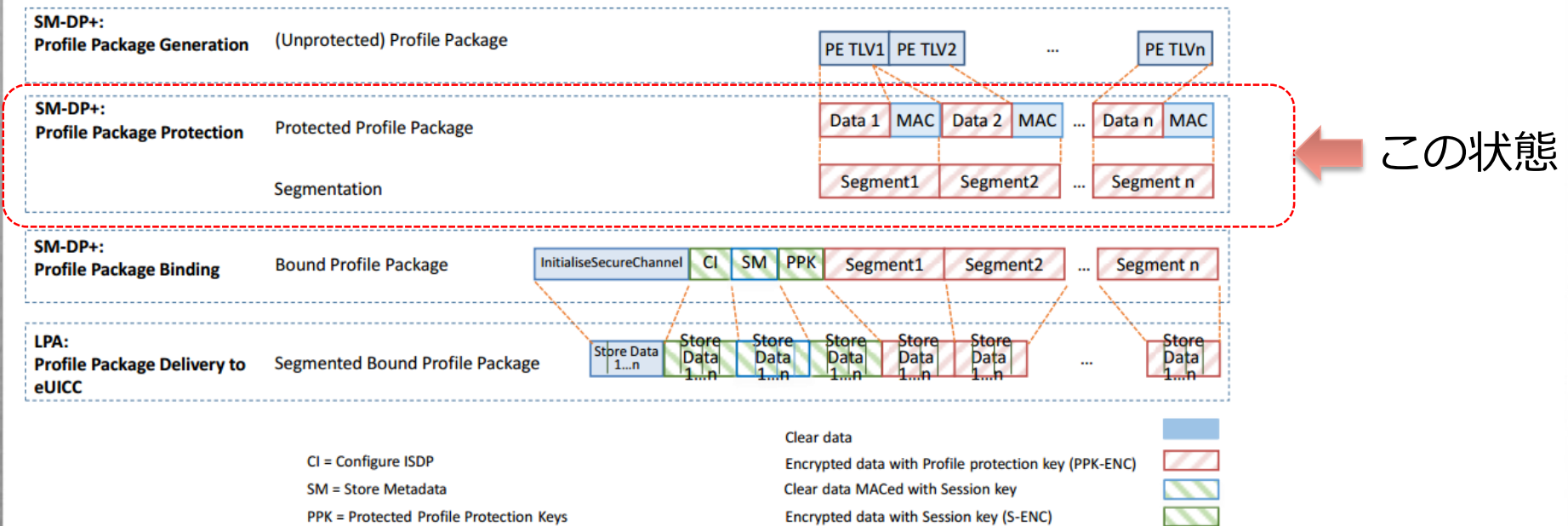


Figure 4: Profile Package stage Description

SGP.22より引用

eSIMについて

- IIJ MVNOインフラ概要
- IIJ フルMVNOサービス領域
- eSIMとは？
- IIJ PoCについて
- eSIMの仕組みについて
 - プロファイルのDL
 - SIMプロファイルとは
 - eUICCとは
 - eSIMのセキュリティの仕組み
 - LPAとは
- まとめ

eUICCとは - 1

• eUICCの機能概要 - 1

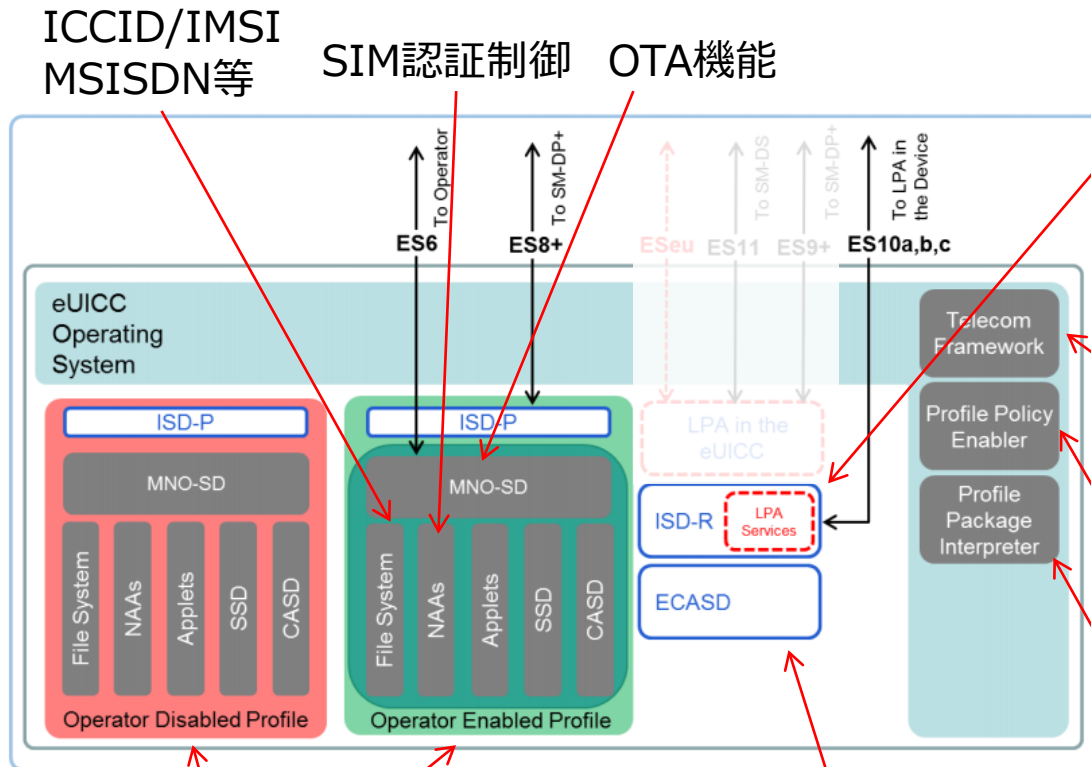


Figure 2: Schematic Representation of the eUICC
SGP.21より引用

端末(LPA)の司令に基づきプロファイル制御を担う根幹部分

- プロファイルの一覧確認
- プロファイルの有効/無効/削除
- プロファイルのDL

などなど

NAA向けSIM認証機能の提供等

SIMプロファイルに設定されているポリシーに基づいた制御を実施

- プロファイル無効化不可
- プロファイル削除不可

SIMプロファイルデータを解析して、ISD-Pのプロファイルデータとして展開する機能

SIMプロファイルを格納
同時に1つのプロファイルしか
アクティブにできない

公開鍵/秘密鍵が格納
されている

eUICCとは - 2

• eUICCの機能概要 - 2

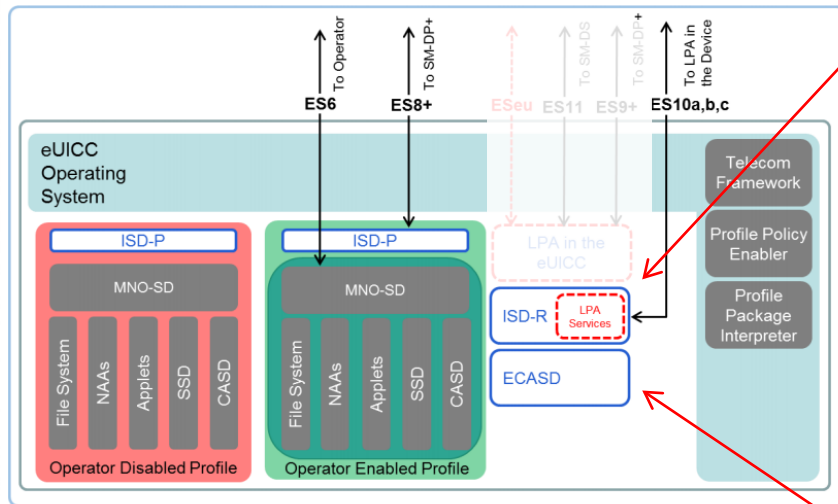


Figure 2: Schematic Representation of the eUICC
SGP.21より引用

カードが持つ設定値

- EID(eUICC-ID)
 - 32桁のユニークな識別子
- RAT(Rule Authorization Table)
 - プロファイル無効化/削除禁止制御
- Default SM-DP+アドレス
- SM-DSアドレス
 - プロファイル自動DLに利用

証明書/秘密鍵

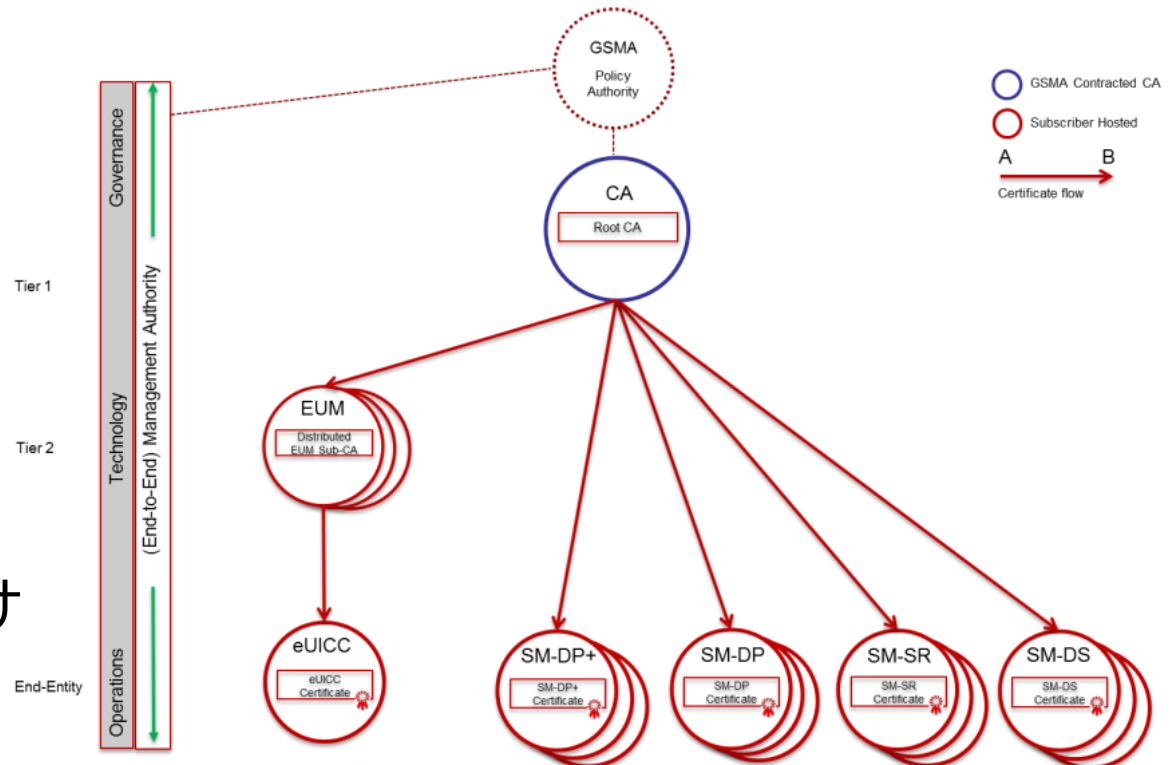
- Root CI証明書
 - SM-DP+証明書の正当性確認
- EUM証明書(中間証明書)
- eUICC証明書, 秘密鍵
 - EID
 - eUICC自身の製造元とその正当性の証明
 - プロファイル暗号化等

eSIMについて

- IIJ MVNOインフラ概要
- IIJ フルMVNOサービス領域
- eSIMとは？
- IIJ PoCについて
- eSIMの仕組みについて
 - プロファイルのDL
 - SIMプロファイルとは
 - eUICCとは
 - eSIMのセキュリティの仕組み
 - LPAとは
- まとめ

eSIMのセキュリティの仕組み - 1

- SM-DP+/eUICCの正当性確認や暗号化のため、公開鍵認証基盤 X.509 を採用(WebのSSL/TLS等と同じやつ)
- GSMAが認証基盤を管理
- SM-DP+サーバを立てる場合や、eUICCを発行するには、GSMA Root CI(CA)で自身の証明書にサインをする必要があるが、このためにはGSMAの認証を受ける必要がある



SGP.14 2.3 PKI Participants から引用

eSIMのセキュリティの仕組み - 2

• 認証取得事業者一覧

<https://www.gsma.com/aboutus/workinggroups/working-groups/fraud-security-group/security-accreditation-scheme/sas-accredited-sites-list>

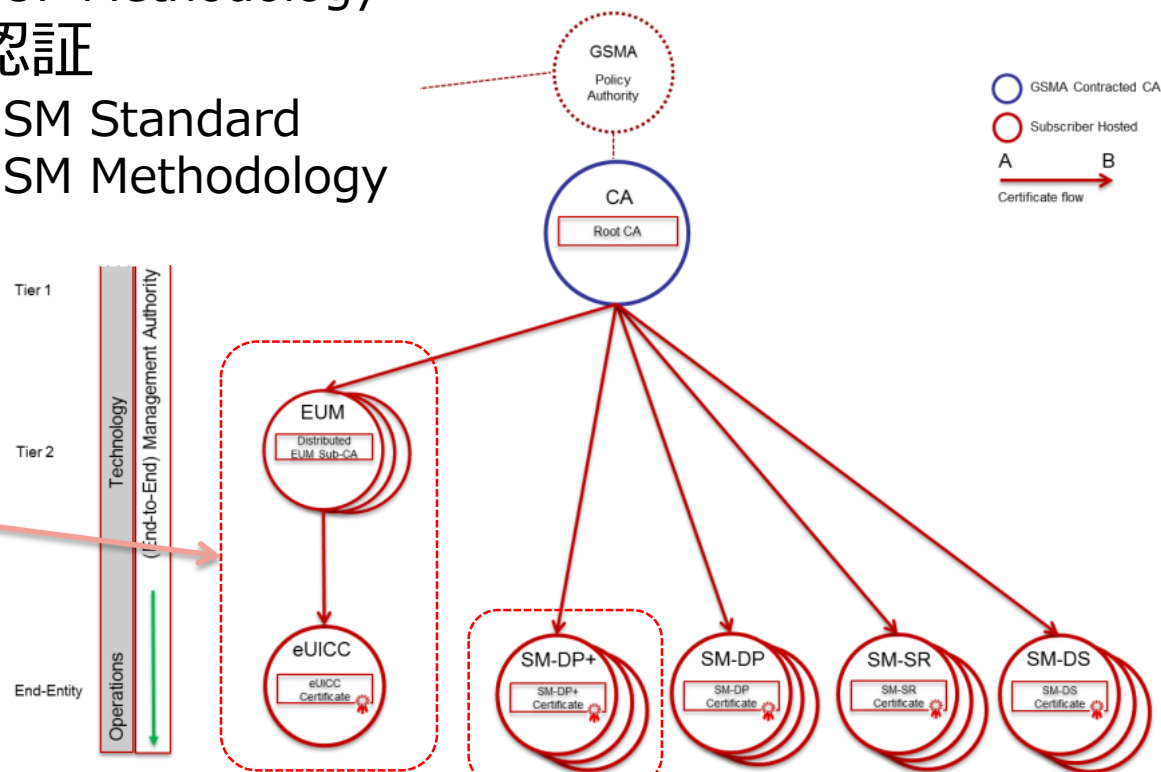
• SIMベンダー(eUICC)のための認証

- GSMA FS.04 - SAS-UP Standard
- GSMA FS.05 - SAS-UP Methodology

• SM-DP+のための認証

- GSMA FS.08 - SAS-SM Standard
- GSMA FS.09 - SAS-SM Methodology

eUICCは量産するので中間認証局(EUM)で証明を受けて、個々のeUICCはEUMで署名する



SGP.14 2.3 PKI Participants から引用

eSIMのセキュリティの仕組み - 3

- それぞれが持つ証明書と秘密鍵の情報

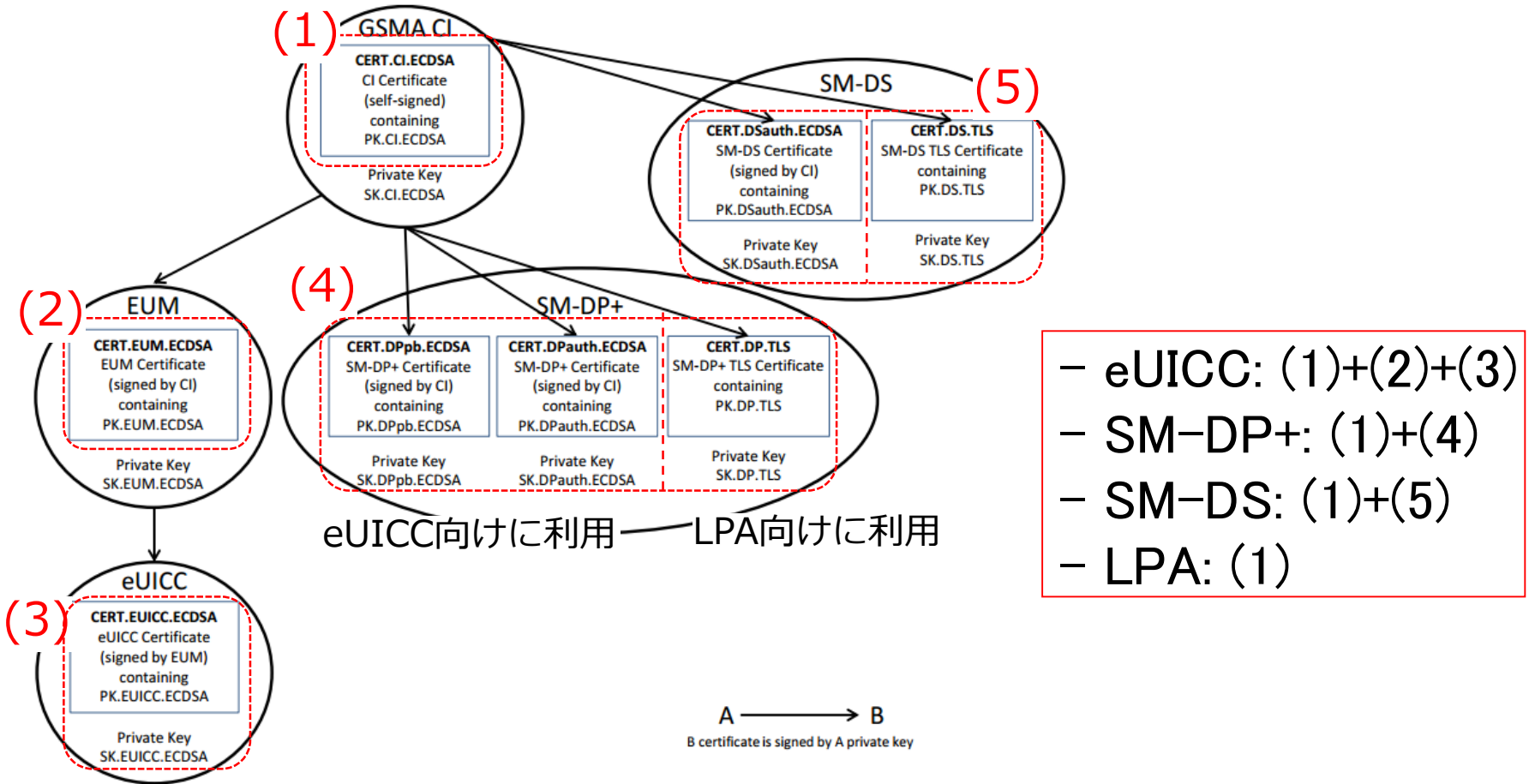


Figure 30: Certificate Chains

SGP.22 4.5.2 Certificatesから引用

eSIMについて

- IIJ MVNOインフラ概要
- IIJ フルMVNOサービス領域
- eSIMとは？
- IIJ PoCについて
- eSIMの仕組みについて
 - プロファイルのDL
 - SIMプロファイルとは
 - eUICCとは
 - eSIMのセキュリティの仕組み
 - LPAとは
- まとめ

LPAとは - 1

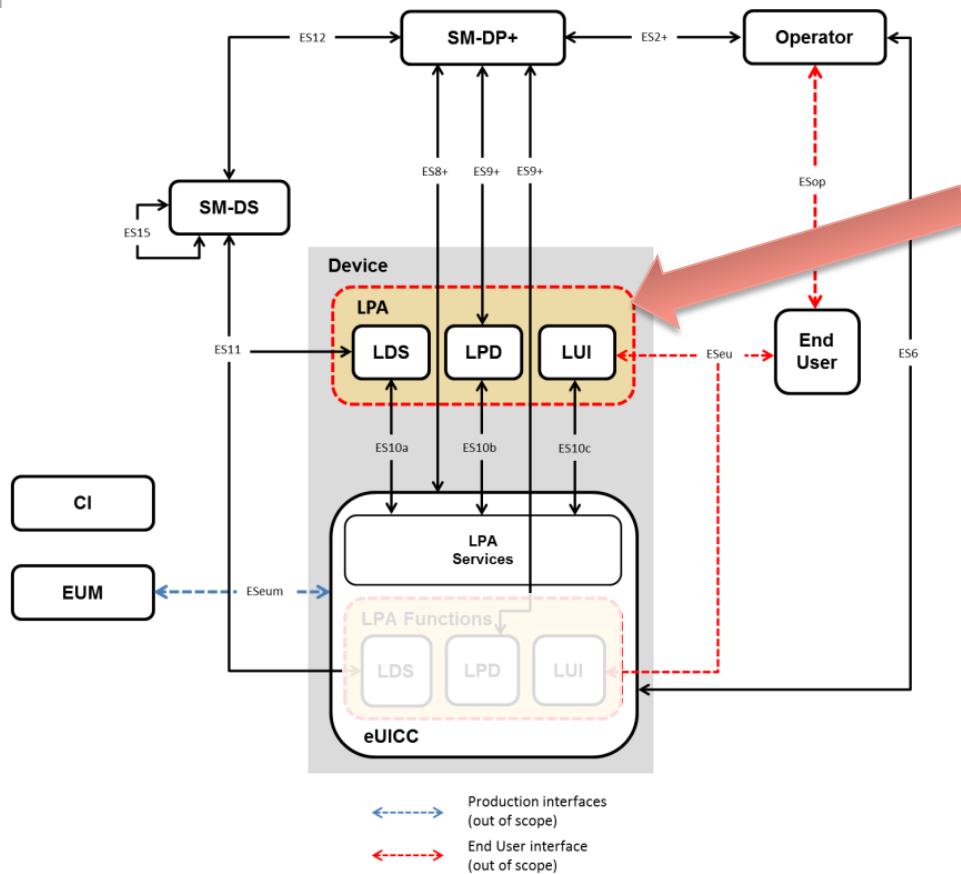


Figure 1: Remote SIM Provisioning System Architecture
SGP.21より引用

LPA(Local Profile Assistant)はユーザのプロファイル管理に関する部分。

3種類の機能に分類される。

- LUI: ユーザからの支持でプロファイルの管理を実施
- LPD: SM-DP+からプロファイルをダウンロードして、eUICCにデータを転送するproxy機能
- LDS: SM-DSに問い合わせ、自身のeSIM(EID)宛にイベントがないかを確認する

LPAとは - 2 / LUIの例

← 設定

ホーム

設定の検索

ネットワークとインターネット

状態

Wi-Fi

携帯電話

ダイヤルアップ

VPN

機内モード

モバイル ホットスポット

データ使用状況

プロキシ

携帯電話

このSIMカードの携帯データネットワークを使う

SIM 1

IIJ (HSDPA)
切断済み

接続

Windows でこの接続を管理

携帯データ ネットワークを使用するたびに、手動で接続する必要があります。

データ ローミング オプション

ローミングを許可する

サービス契約の内容によっては、データ ローミングを使用すると料金が割り増しになる場合があります。

[eSIM プロファイルの管理](#)

[詳細オプション](#)

[携帯データネットワークを使えるアプリを選ぶ](#)

Wi-Fi ではなく携帯ネットワークを使用する

Wi-Fi の状態が悪い場合

Wi-Fi 経由のインターネット接続状態が悪い場合は、自動的に携帯データ ネットワークに切り替えます。これにはご使用のデータ通信プランが使用されるため、料金がかかる可能性があります。

関連設定

[アダプターのオプションを変更する](#)

[ネットワークと共有センター](#)

[Windows ファイアウォール](#)

[詳細情報](#)

質問がありますか?
[ヘルプを表示](#)

Windows をより良い製品に
[フィードバックの送信](#)

ここからLUIへ

ここに入力して検索

18:24
2018/11/19

LPAとは - 3 / LUIの例

← 設定

— □ ×

🏠 eSIM プロファイルの管理

eSIM プロファイル

携帯電話会社の eSIM プロファイルを追加します。

質問がありますか？

[ヘルプを表示](#)

+ 新しいプロファイルを追加します

プロファイルの追加

IIJ アクティブ



プロファイルの管理

IIJ

サインイン要件

eSIM 設定を管理するためにサインインを求める。

オフ

eSIM プロファイルを追加、削除、または管理するためにサインインする必要はありません。

eSIM のプロパティ



🔍 ここに入力して検索



18:24
2018/11/19



LPAとは - 4 / LUIの例

← 設定

- □ ×

🏠 eSIM プロファイルの管理


eSIM プロファイル

携帯電話会社の eSIM プロファイルを追加します。

質問がありますか？

[ヘルプを表示](#)

+ 新しいプロファイルを追加します

 IIJ
アクティブ
IIJ
ICCID:8981030
使用中止 名前を編集 削除



プロファイルの
無効化/削除等

サインイン要件

eSIM 設定を管理するためにサインインを求める。

オフ

eSIM プロファイルを追加、削除、または管理するためにサインインする必要はありません。

eSIM のプロパティ

ここに入力して検索



LPAとは - 5 / LUIの例

← 設定

- □ ×

🏠 eSIM プロファイルの管理

eSIM プロファイル

携帯電話会社の eSIM プロファイルを追加します

+ 新しいプロファイルを追加します

 IIJ
アクティブ
IIJ
ICCID:898103
[使用中] [名前]

 IIJmio

サインイン要件

eSIM 設定を管理するためにサインインを求めます。

 オフ

eSIM プロファイルを追加、削除、または管理するためにサインインする必要はありません。

eSIM のプロパティ

どのような方法で新しいプロファイルを追加しますか？

- 使用可能なプロファイルの検索
- 携帯電話会社から提供されたアクティベーションコードを入力する

次へ

キャンセル

質問がありますか？

[ヘルプを表示](#)

プロフィール追加
をActivation Codeで

LPAとは - 6 / LUIの例

The screenshot shows a Windows application window titled "ファイルの管理" (File Management). The main content area is titled "QRコードのスキャン" (QR Code Scanning) and "カメラの選択" (Camera Selection). A dropdown menu shows "Microsoft BarcodeScanner (Microsoft Camera Rear)". A QR code is displayed in the center. Below it, the "アクティベーションコード" (Activation Code) field contains "1\$ij- :com\$4PT HVZ". At the bottom are "次へ" (Next) and "キャンセル" (Cancel) buttons. On the left, a context menu is open with options like "元のサイズに戻す(R)", "移動(M)", "サイズ変更(S)", "最小化(N)", "最大化(X)", and "閉じる(C) Alt+F4". On the right, there are links for "質問がありますか?" (Do you have a question?) and "ヘルプを表示" (Show help). Two red arrows point from text boxes on the right to the QR code and the activation code field.

設定

元のサイズに戻す(R)
移動(M)
サイズ変更(S)
最小化(N)
最大化(X)
閉じる(C) Alt+F4

ファイルの管理

携帯電話会社の eSIM プロファイルを追加します

新しいプロファイルを追加します

IIJ IIJ アクティブ
IIJmio IIJ

サインイン要件

eSIM 設定を管理するためにサインインを求める。

オフ

eSIM プロファイルを追加、削除、または管理する
ありません。

eSIM のプロパティ

QRコードのスキャン

カメラの選択

Microsoft BarcodeScanner (Microsoft Camera Rear)

アクティベーションコード

1\$ij- :com\$4PT HVZ

次へ キャンセル

質問がありますか?
ヘルプを表示

QRコード
読み取り

Activation
Code直接
入力

ここに入力して検索

18:27
2018/11/19

LPAとは - 7 / LUIの例

LUIの問題点: QRコード読み込み問題



ファイルの管理

携帯電話会社の eSIM プロファイルを追加します

+ 新しいプロファイルを追加します

IIJ アクティブ

IIJmio

サインイン要件

eSIM 設定を管理するためにサインインを求める。

オフ

eSIM プロファイルを追加、削除、または管理する
ありません。

eSIM のプロパティ



QRコード読み込みは外部カメラを前提としているものが多数。

この端末自身でeSIMサービスを契約する場合に、ブラウザーに表示されたQRコードは、カメラでは取り込めない。

文字列のActivation codeを入力する必要あり。

独自仕様アプリでこの問題を回避している場合が多い



LPAとは - 8 / LPDの例

- LPDの役割を理解するために、Activation Code(QR)を利用してプロファイルダウンロードする場合のシーケンスで確認
- 大まかに分けると下記のフェーズに分かれる
 1. SM-DP+側とeUICC側の相互認証による正当性の確認
 2. SM-DP+から暗号化したプロファイルにダウンロード
 3. プロファイルの有効化

SM-DP+側は HTTPS/JSONの通信で、DERをBase64変換して送受信

eUICC側とはDER(ASN.1)で送受信

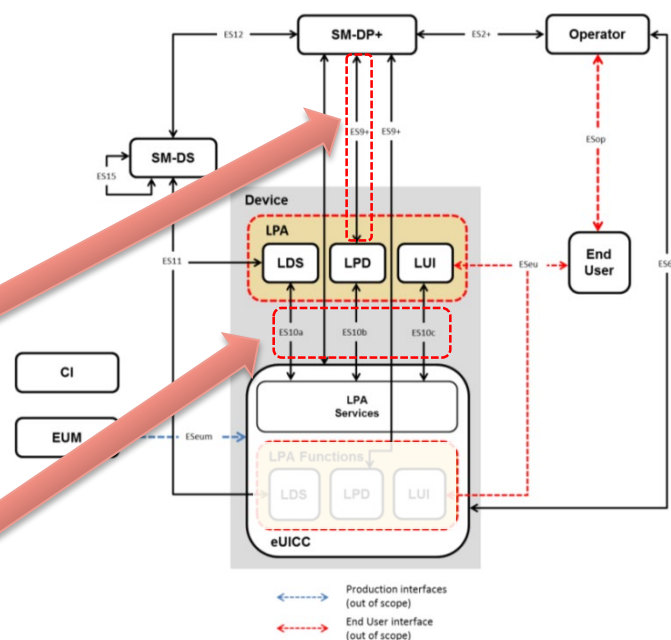


Figure 1: Remote SIM Provisioning System Architecture
SGP.21より引用

LPAとは - 9 / LPDの例

SM-DS+

MNO(IIJ)

IIJ Profile
Available

ユーザから契約申し込み来た

ES2+.DownloadOrder

```
HTTP POST /gsma/rsp2/es2plus/downloadOrder HTTP/1.1
Host: smdp.iij.ad.jp
X-Admin-Protocol: gsma/rsp/v2.2.0
Content-Type: application/json
Content-Length: XXX
{
  "header" : {
    "functionRequesterIdentifier" : "IIJ-IIJ",
    "functionCallIdentifier" : "IIJ-567"
  },
  "iccid" : "898103000000xxxxxxF",
}
```

ユーザに割り当てるiccidのSIMプロファイル確保可能か確認。

IIJ Profile
Allocated

ES2+.DownloadOrder response

```
HTTP/1.1 200 OK
X-Admin-Protocol: gsma/rsp/v2.2.0
Content-Type: application/json
Content-Length: XXX
{
  "header" : {
    "functionExecutionStatus" : {
      "status" : "Executed-Success"
    }
  },
  "iccid" : "898103000000xxxxxxF",
}
```

OKならば、確保済み状態になるが、この時点ではまだDLはできない

(次へ続く)

LPAとは - 10 / LPDの例

SM-DS+

MNO(IIJ)

ES2+.ConfirmOrder

```
HTTP POST /gsma/rsp2/es2plus/confirmOrder HTTP/1.1
Host: smdp.ij.ad.jp
X-Admin-Protocol: gsma/rsp/v2.2.0
Content-Type: application/json
Content-Length: XXX
{
  "header" : {
    "functionRequesterIdentifier" : "IJ-IJ",
    "functionCallIdentifier" : "IJ-567"
  },
  "releaseFlag": true,
  "iccid" : "898103000000xxxxxxF",
}
```

確保したプロファイルをダウンロード可能な状態にする

OKならばActivation Code生成に必要な
- Matching ID
- SM-DP+アドレス
を取得。

(注) MNO側が Matching ID をしている
すことも可能

IJ Profile
Released

ES2+.ConfirmOrder response

```
HTTP/1.1 200 OK
X-Admin-Protocol: gsma/rsp/v2.2.0
Content-Type: application/json
Content-Length: XXX
{
  "header" : {
    "functionExecutionStatus" : {
      "status" : "Executed-Success"
    }
  },
  "matchingId": "2C86-927E-XXXX-XXXX",
  "smdpAddress": "ij-xxxxxxxx.com"
}
```

QRコードを生成してユーザに渡す。

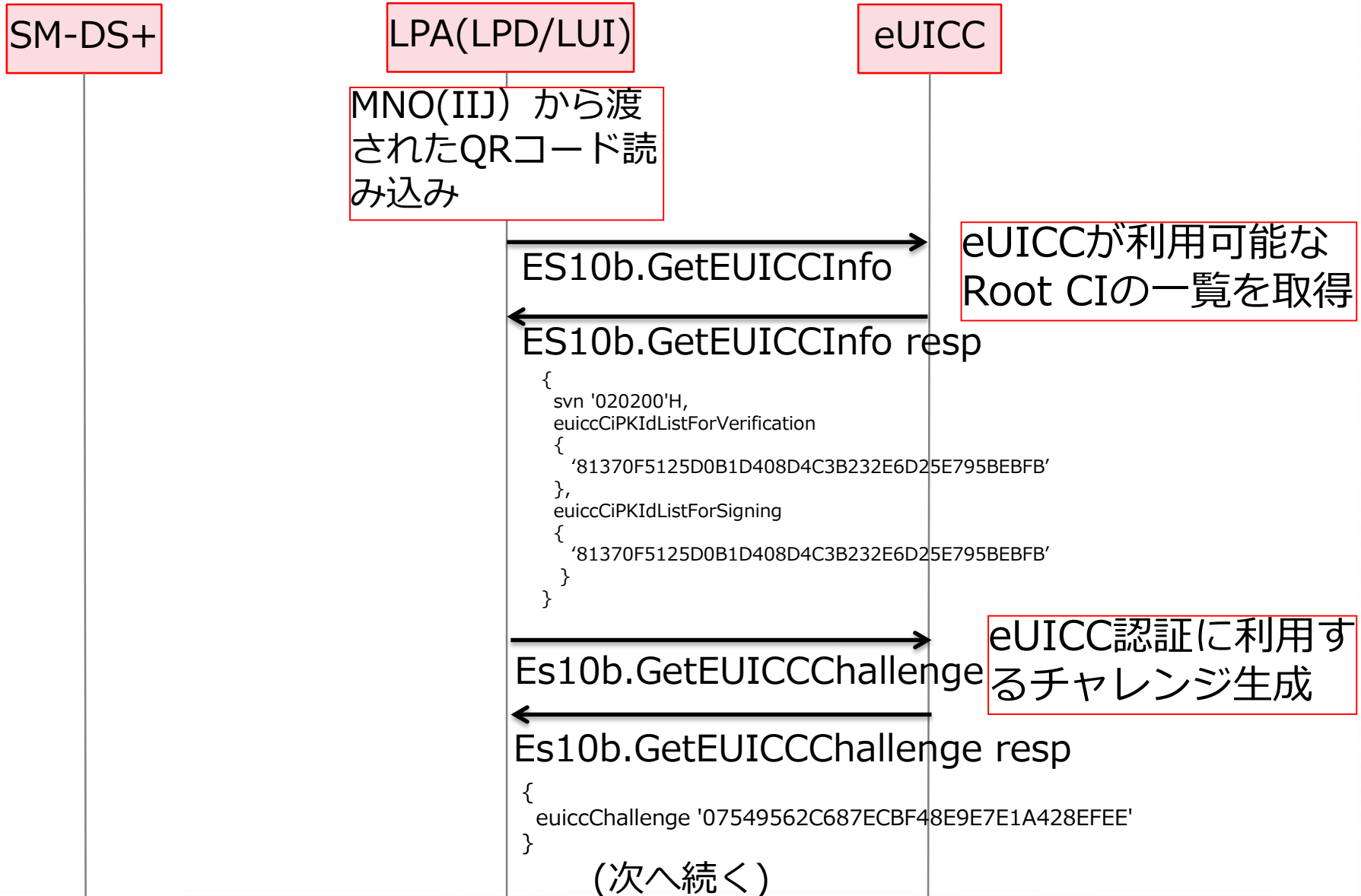
例)

LPA:1\$ij-xxxxxxxx.com\$2C86-927F-XXXX-XXXX

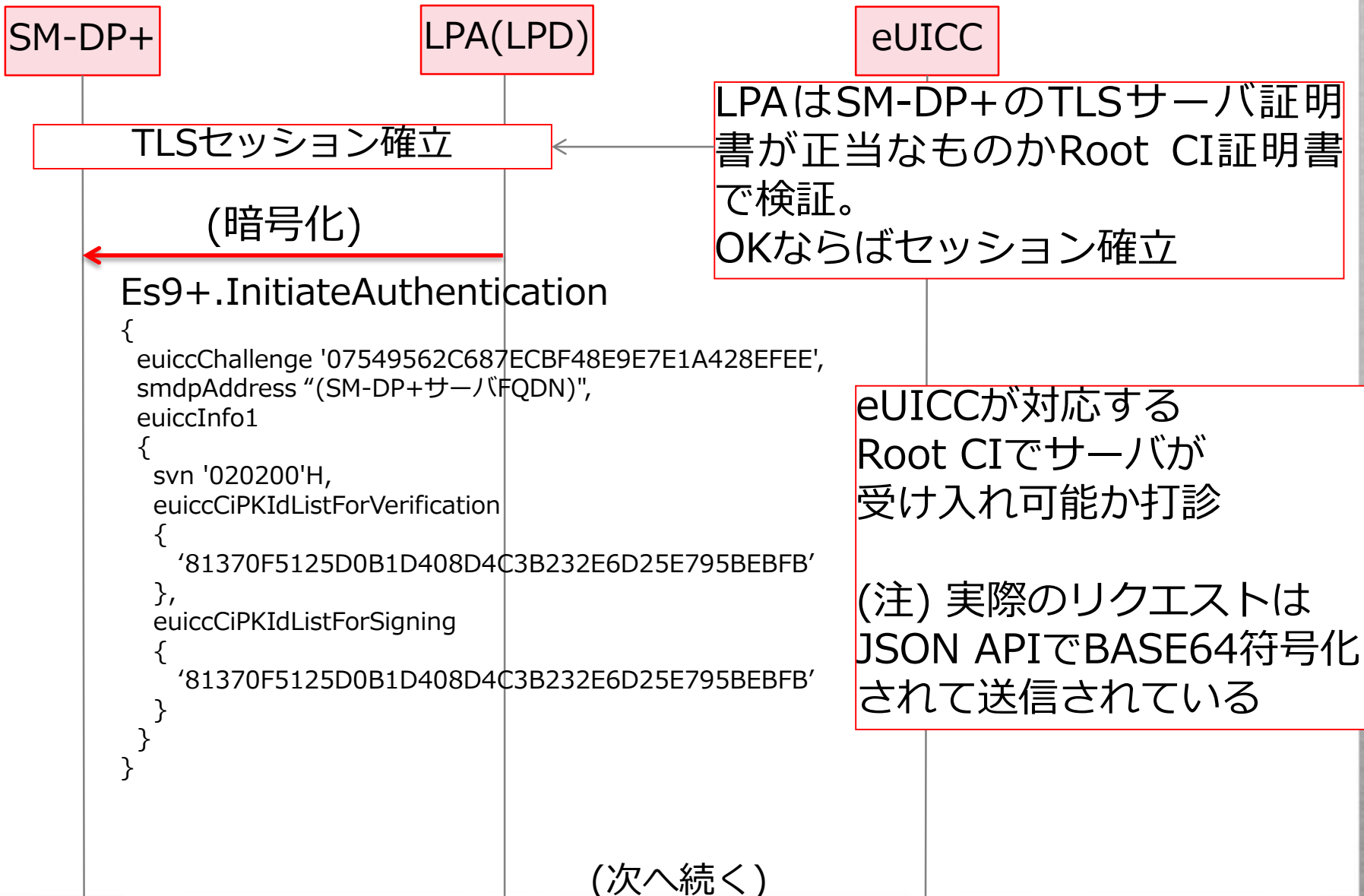


QRコード生成 (次へ続く)

LPAとは - 11 / LPDの例



LPAとは - 12 / LPDの例



LPAとは - 13 / LPDの例

SM-DP+

LPA(LPD)

eUICC

Es9+.InitiateAuthentication response

initiateAuthenticationOk :

```
{
  transactionId 'E0FD290C187D1348912798F7DB1B1959',
  serverSigned1
  {
    transactionId 'E0FD290C187D1348912798F7DB1B1959',
    euiccChallenge '07549562C687ECBF48E9E7E1A428EFEE',
    serverAddress "(SM-DP+サーバFQDN)",
    serverChallenge 'C24D048AA07B86019239DC14077AA5FF'
  },
  serverSignature1 '(サーバからの応答の改ざん検出のためのsignature)',
  euiccCiPKIdToBeUsed '81370F5125D0B1D408D4C3B232E6D25E795BEBFB',
  serverCertificate
  {
    (サーバ証明書情報 Cert.DPauth.ECDSA /長いので省略)
  }
}
```

SM-DP+が対応可能な
Root CIを返す。
相互認証に必要なサーバ
側の証明書情報を送信

(次へ続く)

LPAとは - 14 / LPDの例

SM-DP+

LPA(LPD)

eUICC

Es10b.AuthenticateServer

```

{
  serverSigned1
  {
    transactionId 'E0FD290C187D1348912798F7DB1B1959',
    euiccChallenge '07549562C687ECBF48E9E7E1A428EFEE',
    serverAddress "(SM-DP+サーバFQDN)",
    serverChallenge 'C24D048AA07B86019239DC14077AA5FF'
  },
  serverSignature1 '(サーバからの応答の改ざん検出のためのsignature)',
  euiccCpKeyIdToBeUsed '81370F5125D0B1D408D4C3B232E6D25E795BEBFB',
  serverCertificate
  {
    (サーバ証明書情報 Cert.DPauth.ECDSA /長いので省略)
  },
  ctxParams1 ctxParamsForCommonAuthentication :
  {
    matchingId "2C86-927E-XXXX-XXXX",
    deviceInfo
    {
      tac '00000000'H,
      deviceCapabilities
      {
      }
    }
  }
}

```

LPAは、SM-DP+からの
Es9+.InitiateAuthentication
Responseをほぼそのまま
eUICCに転送。
その際に、Matching ID等の
追加情報を付加

(次へ続く)

LPAとは - 15 / LPDの例

SM-DP+

LPA(LPD)

eUICC

Es10b.AuthenticateServer response

```

authenticateResponseOk :
{
  euiccSigned1
  {
    transactionId 'E0FD290C187D1348912798F7DB1B1959'H,
    serverAddress "(SM-DP+サーバ(FQDN))",
    serverChallenge 'C24D048AA07B86019239DC14077AA5FF'H,
    euiccInfo2
    {
      profileVersion '020x00'H,
      svn '020200'H,
      euiccFirmwareVer 'xxxxxx'H,
      extCardResource '81010082040008063A830400001C08'H,
      uiccCapability { usimSupport, isimSupport, csimSupport, akaMilenage, akaCave, akaTuak128, akaTuak256, gbaAuthen1Sim,
eapClient, javacard, multipleUsimSupport, multipleIsimSupport },
      ts102241Version '090200'H,
      globalplatformVersion '020300'H,
      rspCapability { additionalProfile, testProfileSupport },
      euiccCipKIdListForVerification
      {
        '81370F5125D0B1D408D4C3B232E6D25E795BE8FB'
      },
      euiccCipKIdListForSigning
      {
        '81370F5125D0B1D408D4C3B232E6D25E795BE8FB'
      },
      forbiddenProfilePolicyRules { pprUpdateControl },
      ppVersion '000001'H,
      sasAcreditationNumber "XXXXXXXXXXXXXXXX",
      certificationDataObject
      {
        platformLabel "1.2.840.1234XXX/myPlatformLabel",
        discoveryBaseURL "https://mycompany.com/myDLOARegistrar"
      }
    },
    ctxParams1 ctxParamsForCommonAuthentication :
    {
      matchingId "2C86-927E-XXXX-XXXX",
      deviceInfo
      {
        tac '00000000'H,
        deviceCapabilities
        {
          {
          }
        }
      }
    },
    euiccSignature1 '(メッセージ改ざん防止のsignature)',
    euiccCertificate
    {
      (eUICC証明書/この中にEID含む)
    },
    eumCertificate
    {
      (EUM(SIMベンダー)証明書)
    }
  }
}

```

eUICCは自身の持つRoot CI
証明書で、SM-DP+サーバ証
明書が正当なものか検証。

OKならば、応答に

- Matching ID
- カードの対応機能等
- eUICC証明書(EID含む)
- EUM証明書
(SIMベンダー中間CA)

を含めて、カード側の正当性
認証を依頼

(次へ続く)

LPAとは - 16 / LPDの例

SM-DP+

LPA(LPD)

eUICC

←

Es9+.AuthenticateClient

```
{
  transactionId 'E0FD290C187D1348912798F7DB1B1959'H,
  authenticateServerResponse authenticateResponseOk
  {
    euiccSigned1
    {
      transactionId 'E0FD290C187D1348912798F7DB1B1959'H,
      serverAddress "(SM-DP+サーバ(FQDN))",
      serverChallenge 'C24D048AA07B86019239DC14077AA5FF'H,
      euiccInfo2
      {
        profileVersion '020100'H,
        svn '020200'H,
        euiccFirmwareVer 'xxxxx'H,
        extCardResource '81010082040008063A830400001C08'H,
        uiccCapability { usimSupport, isimSupport, csimSupport, akaMilenage, akaCave, akaTuak128, akaTuak256, gbaAuthenISim, eapClient, javacard,
        multipleUsimSupport, multipleIsimSupport },
        ts102241Version '090200'H,
        globalplatformVersion '020300'H,
        rspCapability { additionalProfile, testProfileSupport },
        euiccCiPKIdListForVerification
        {
          '81370F5125D0B1D408D4C3B232E6D25E795BEBFB'
        },
        euiccCiPKIdListForSigning
        {
          '81370F5125D0B1D408D4C3B232E6D25E795BEBFB'
        },
        forbiddenProfilePolicyRules { pprUpdateControl },
        ppVersion '000001'H,
        sasAcreditationNumber "XXXXXXXXXXXXXXXXXX",
        certificationDataObject
        {
          platformLabel "1.2.840.1234XXX/myPlatformLabel",
          discoveryBaseUrl "https://mycompany.com/myDLOARegistrar"
        }
      },
      ctxParams1 ctxParamsForCommonAuthentication :
      {
        matchingId "2C86-927E-XXXX-XXXX",
        deviceInfo
        {
          tac '00000000'H,
          deviceCapabilities
          {
            {
            }
          }
        }
      },
      euiccSignature1 '(メッセージ改ざん防止のsignature)',
      euiccCertificate
      {
        (eUICC証明書/この中にEID含む)
      },
      eumCertificate
      {
        (EUM(SIMヘンダー)証明書)
      }
    }
  }
}
```

Es10b.Authenticate
Server responseの内容をそのままJSONに変換して、SM-DP+へ

(次へ続く)

LPAとは - 17 / LPDの例

SM-DP+

LPA(LPD)

eUICC

IIJ Profile
Released

Es9+.AuthenticateClient Response

```
authenticateClientOk :
{
  transactionId 'E0FD290C187D1348912798F7DB1B1959',
  profileMetaData
  {
    iccid '981830000000XXXXXXFX'H,
    serviceProviderName "IIJ",
    profileName "",
    iconType png,
    icon '(hex binary data)'
  },
  smdpSigned2
  {
    transactionId 'E0FD290C187D1348912798F7DB1B1959',
    ccRequiredFlag FALSE
  },
  smdpSignature2 '(メッセージ改ざん防止signature)',
  smdpCertificate
  {
    (プロファイル暗号化用サーバ証明書, Cert.DPpb.ECDSA)
  }
}
```

サーバ側でeUICCの正当性の確認、および、Matching IDに紐づくプロファイルが存在するか確認。

OKの場合は、LPA上でのDL対象プロファイル情報をMeta Dataとして送る。

また、プロファイル暗号化のためのサーバ証明書(Cert.DPpb.ECSAD)を送信。

(次へ続く)

LPAとは - 18 / LPDの例

SM-DP+

LPA(LPD)

eUICC

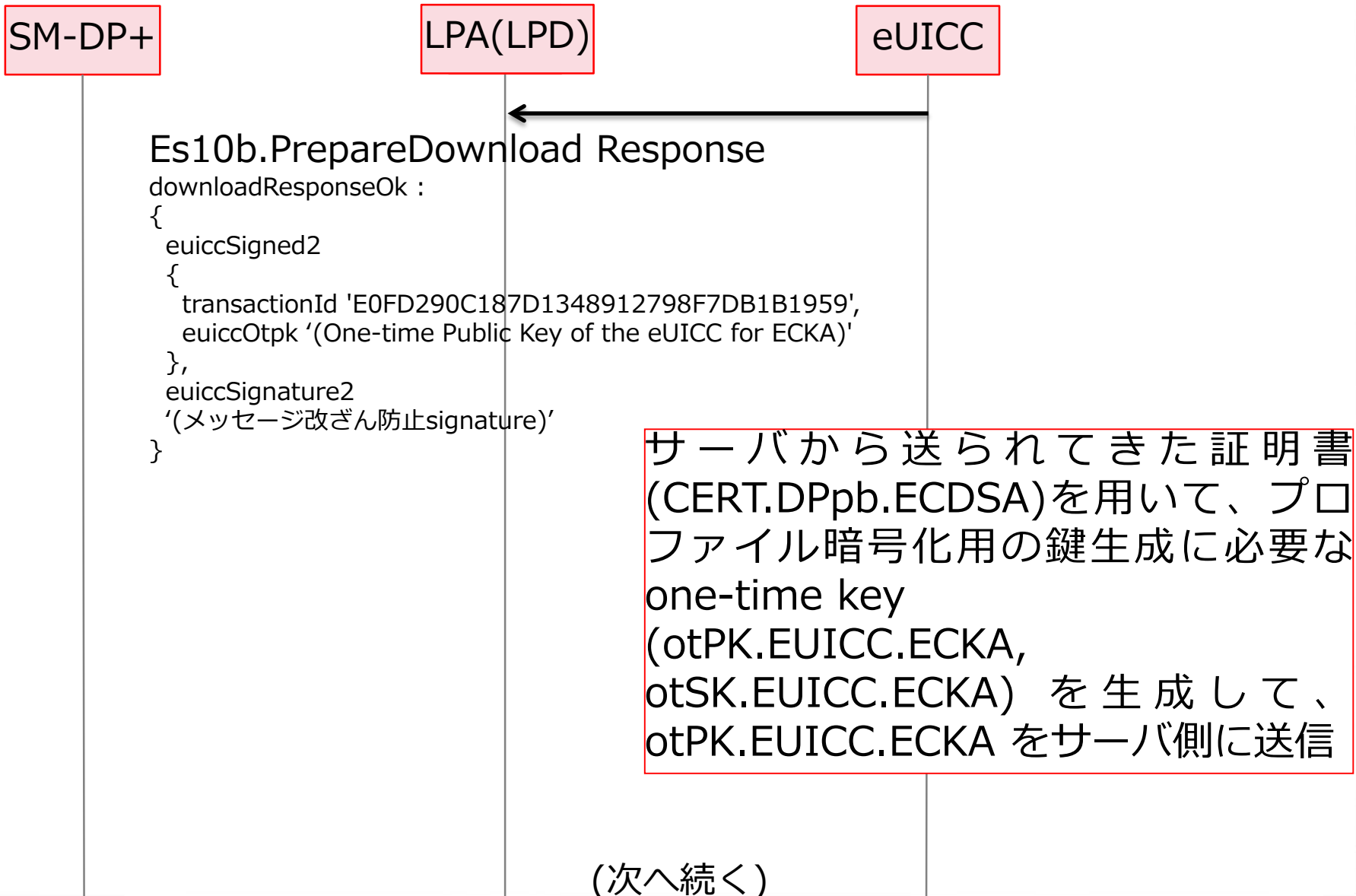
Es10b.PrepareDownload

```
{
  smdpSigned2
  {
    transactionId 'E0FD290C187D1348912798F7DB1B1959',
    ccRequiredFlag FALSE
  },
  smdpSignature2 '(メッセージ改ざん防止signature)',
  smdpCertificate
  {
    (プロファイル暗号化用サーバ証明書, Cert.DPpb.ECDSA)
  }
}
```

Es9+.AuthenticateClient Response の
smdpSigned2 以降の
データをeUICCに転送

(次へ続く)

LPAとは - 19 / LPDの例



(次へ続く)

LPAとは - 20 / LPDの例

SM-DP+

LPA(LPD)

eUICC

```
Es9+.GetBoundProfilePackage
{
  transactionId 'E0FD290C187D1348912798F7DB1B1959'H,
  prepareDownloadResponse downloadResponseOk :
  {
    euiccSigned2
    {
      transactionId 'E0FD290C187D1348912798F7DB1B1959',
      euiccOtpk '(One-time Public Key of the eUICC for ECKA)'
    },
    euiccSignature2
    '(メッセージ改ざん防止signature)'
  }
}
```

LPA は Es10b.PrepareDownload Response を、そのまま JSON 形式に変換して転送

(次へ続く)

LPAとは - 21 / LPDの例

SM-DP+

LPA(LPD)

eUICC

IIJ Profile
 <-> EID
 Downloaded

Es9+.GetBoundProfilePackage response

```
getBoundProfilePackageOk :
{
  transactionId 'E0FD290C187D1348912798F7DB1B1959'H,
  boundProfilePackage
  {
    initialiseSecureChannelRequest
    {
      remoteOpId installBoundProfilePackage,
      transactionId 'E0FD290C187D1348912798F7DB1B1959'H,
      controlRefTemplate
      {
        keyType '88'H,
        keyLen '10'H,
        hostId '4352545F484F53544944'H
      },
      smdpOtpk '(One-time Public Key of the SM-DP+for ECKA)',
      smdpSign '(メッセージ改ざん防止のためのsignature)'
    },
    firstSequenceOf87
    {
      '(ES8+.ConfigureISDPを暗号化したデータ)'
    },
    sequenceOf88
    {
      '(ES8+.StoreMetadataのデータ)'
    },
    sequenceOf86
    {
      '(Es8+.LoadProfileElementsを暗号化したデータの分割1/4)',
      '(Es8+.LoadProfileElementsを暗号化したデータの分割2/4)',
      '(Es8+.LoadProfileElementsを暗号化したデータの分割3/4)',
      '(Es8+.LoadProfileElementsを暗号化したデータの分割4/4)'
    }
  }
}
```

サ ー バ 証 明 書
 (CERT.DPpb.ECDSA) を用いて、
 プロファイル暗号化用の鍵生成に
 必要な one-time key
 (otPK.DP.ECKA, otSK.DP.ECKA)
 を生成して、 otPK.DP.ECKA を
 eUICC側に送信(eUICC側の復号
 化に必要)

また、暗号化したプロファイル
 データ等をeUICC宛に送信

(次へ続く)

LPAとは - 22 / LPDの例

SM-DP+

LPA(LPD)

eUICC

Es10b.LoadBoundProfilePackage

```

{
  initialiseSecureChannelRequest
  {
    remoteOpId installBoundProfilePackage,
    transactionId 'E0FD290C187D1348912798F7DB1B1959'H,
    controlRefTemplate
    {
      keyType '88'H,
      keyLen '10'H,
      hostId '4352545F484F53544944'H
    },
    smdpOtpk '(One-time Public Key of the SM-DP+for ECKA)',
    smdpSign '(メッセージ改ざん防止のためのsignature)'
  },
  firstSequenceOf87
  {
    '(ES8+.ConfigureISDPを暗号化したデータ)'
  },
  sequenceOf88
  {
    '(ES8+.StoreMetadataのデータ)'
  },
  sequenceOf86
  {
    '(Es8+.LoadProfileElementsを暗号化したデータの分割1/4)',
    '(Es8+.LoadProfileElementsを暗号化したデータの分割2/4)',
    '(Es8+.LoadProfileElementsを暗号化したデータの分割3/4)',
    '(Es8+.LoadProfileElementsを暗号化したデータの分割4/4)'
  }
}

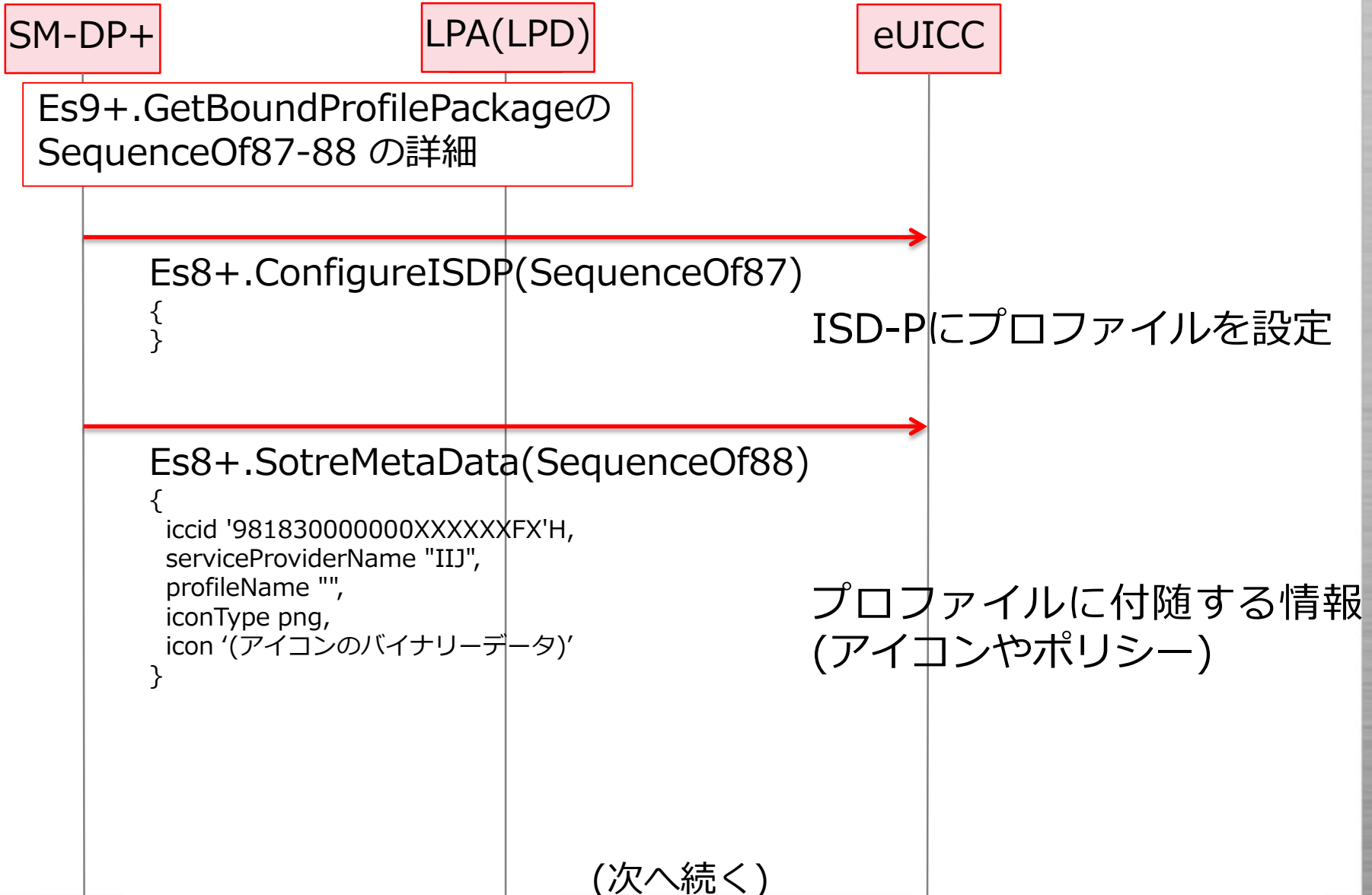
```

LPAEs9+.GetBoundProfilePackage response の内容をほぼそのままeUICCに転送。

LPAはプロファイル部分は暗号化されているので知ることができない。

(次へ続く)

LPAとは - 23 / LPDの例



LPAとは - 24 / LPDの例

SM-DP+

LPA(LPD)

eUICC

Es9+.GetBoundProfilePackageの
SequenceOf87-88 の詳細

Es8+.LoadProfileElements(SequenceOf86)

```
{
  header :
  {
    major-version 2,
    minor-version x,
    profileType "xxxxxxxxxxxxxxxx",
    iccid '8981030000000xxxxxxF'H,
    eUICC-Mandatory-services
    .
    .
    (省略/プロファイルデータ本体が入っている)
  }
}
```

SIMプロファイル本体情報

(次へ続く)

LPAとは - 25 / LPDの例

SM-DP+

LPA(LPD)

eUICC

←

Es10b.LoadBoundProfilePackage response

```
{
  profileInstallationResultData
  {
    transactionId 'E0FD290C187D1348912798F7DB1B1959'H,
    notificationMetadata
    {
      seqNumber 34,
      profileManagementOperation { notificationInstall },
      notificationAddress "(SM-DP+サーバFQDN)",
      iccid '981830000000XXXXXXFX'H
    },
    smdpOid { 2 999 10 },
    finalResult successResult :
    {
      aid 'A0000005591010FFFFFFFFF8900001100'H,
      simaResponse '3007A0053003800100'H
    }
  },
  euiccSignPIR
  '(メッセージ改ざん防止signature)'
}
```

プロファイルのISD-Pへインストールが成功した場合は、成功したことをサーバに通知

(次へ続く)

LPAとは - 26 / LPDの例

SM-DP+

LPA(LPD)

eUICC



Es9+.HandleNotification

profileInstallationResult :

```

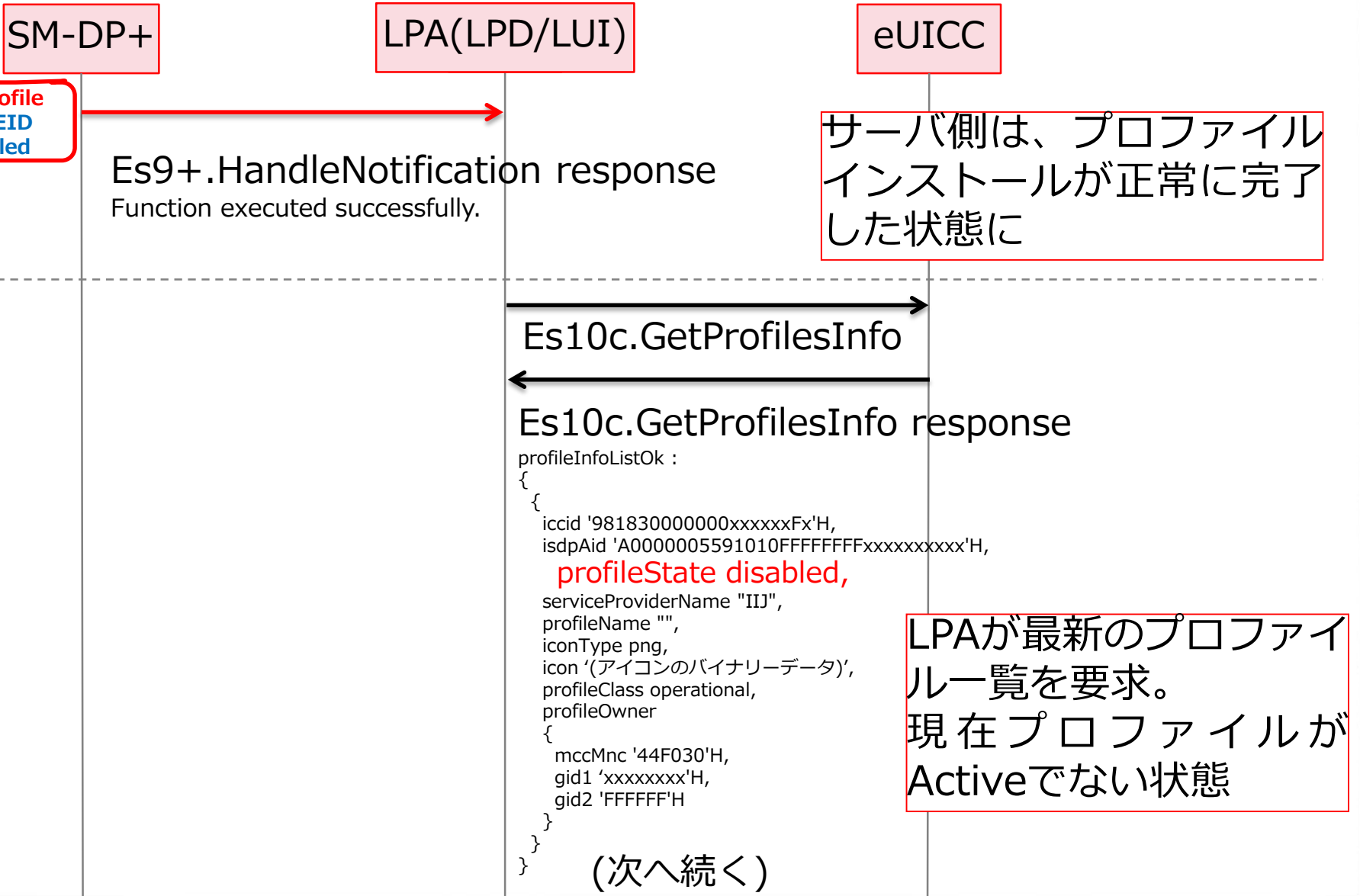
{
  profileInstallationResultData
  {
    transactionId 'E0FD290C187D1348912798F7DB1B1959'H,
    notificationMetadata
    {
      seqNumber 34,
      profileManagementOperation { notificationInstall },
      notificationAddress "(SM-DP+サーバFQDN)",
      iccid '981830000000XXXXXXFX'H
    },
    smdpOid { 2 999 10 },
    finalResult successResult :
    {
      aid 'A0000005591010FFFFFFFFF8900001100'H,
      simaResponse '3007A0053003800100'H
    }
  },
  euiccSignPIR
  '(メッセージ改ざん防止signature)'
}

```

LPA は、
Es10b.LoadBoundProfilePackage responseの内容を
JSON APIに変換して、ほぼ
そのまま転送

(次へ続く)

LPAとは - 27 / LPDの例

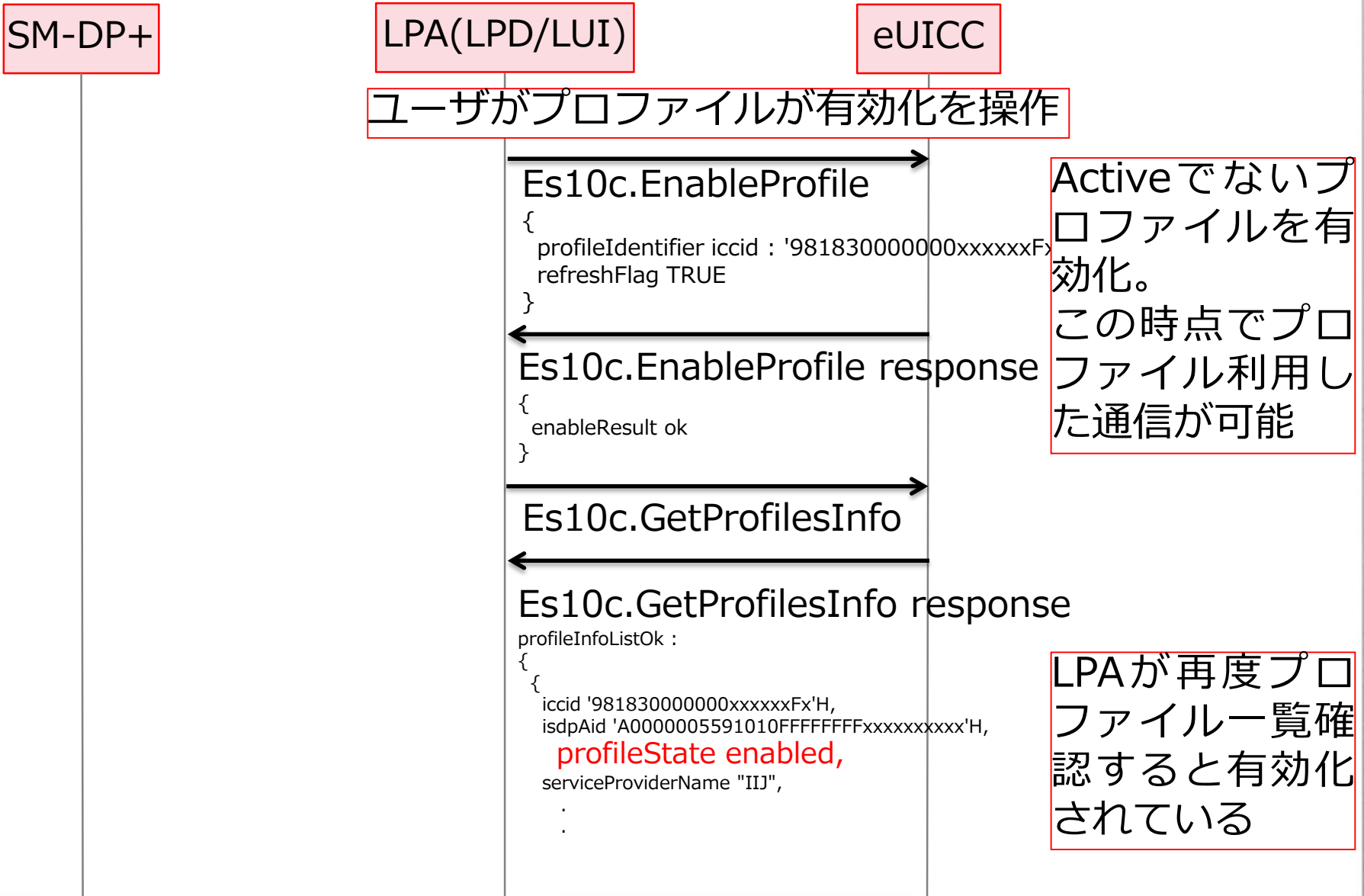


IIJ Profile
-> EID
Installed

サーバ側は、プロファイルインストールが正常に完了した状態に

LPAが最新のプロファイル一覧を要求。
現在プロファイルがActiveでない状態

LPAとは - 28 / LPDの例



LPAとは - 29 / LPDについて

省略

PoCで実施しなかったため
詳細わからず

eSIMについて

- IIJ MVNOインフラ概要
- IIJ フルMVNOサービス領域
- eSIMとは？
- IIJ PoCについて
- eSIMの仕組みについて
- まとめ

まとめ

- 本セッションで下記の内容を共有しました
 - IIJフルMVNOの取り組みについて
 - eSIMに関するIIJ PoCでの実施内容
 - eSIMについて概要とその仕組みを解説
- 2019年春頃を目指して商用サービスを発表出来るようサービス開発を加速させいきます

Lead Initiative

日本のインターネットは1992年、IIJとともに始まりました。以来、IIJグループはネットワーク社会の基盤をつくり、技術力でその発展を支えてきました。インターネットの未来を想い、新たなイノベーションに挑戦し続けていく。それは、つねに先駆者としてインターネットの可能性を切り拓いてきたIIJの、これからも変わることのない姿勢です。IIJの真ん中のIはイニシアティブ

IIJはいつもはじまりであり、未来です。

Ongoing Innovation

本書には、株式会社インターネットイニシアティブに権利の帰属する秘密情報が含まれています。本書の著作権は、当社に帰属し、日本の著作権法及び国際条約により保護されており、著作権者の事前の書面による許諾がなければ、複製・翻案・公衆送信等できません。IIJ、Internet Initiative Japanは、株式会社インターネットイニシアティブの商標または登録商標です。その他、本書に掲載されている商品名、会社名等は各会社の商号、商標または登録商標です。本文中では™、®マークは表示していません。

©Internet Initiative Japan Inc. All rights reserved. 本サービスの仕様、及び本書に記載されている事柄は、将来予告なしに変更することがあります。