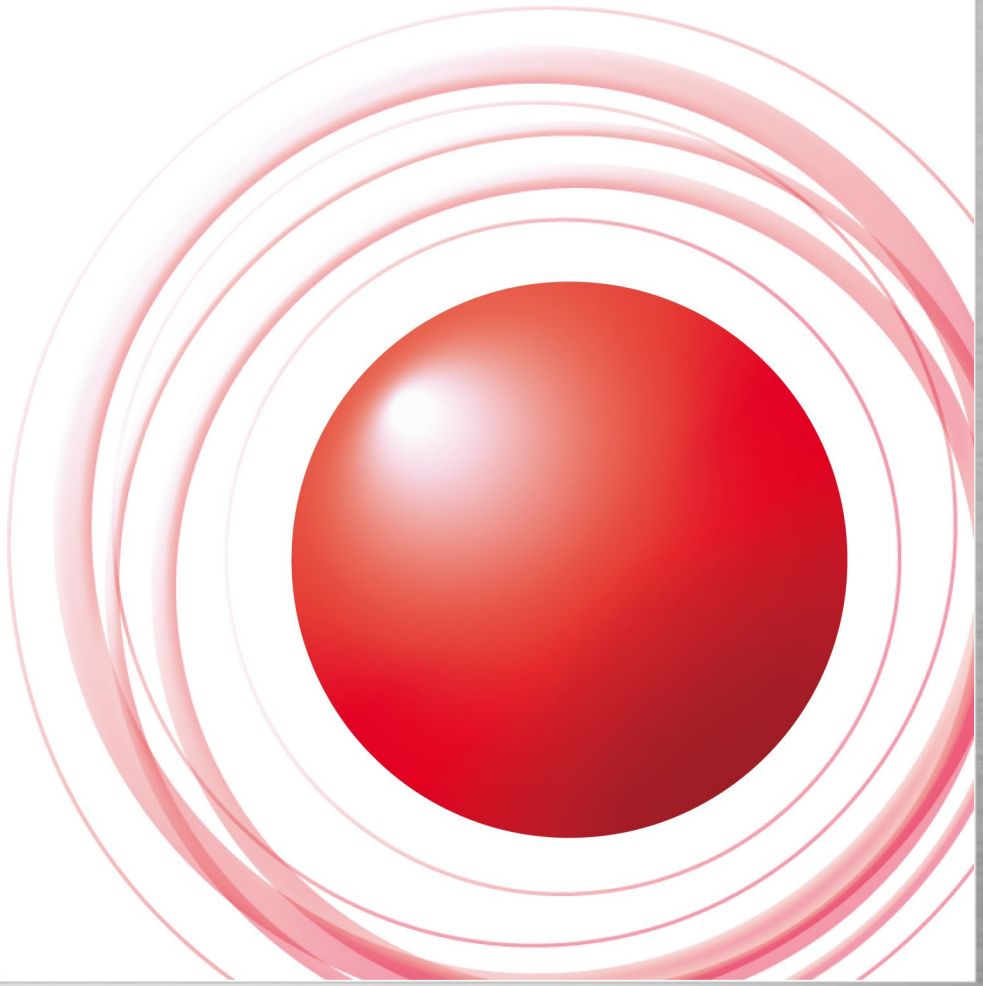
25th Anniversary

eSIMについて

IIJ
Internet Initiative Japan



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

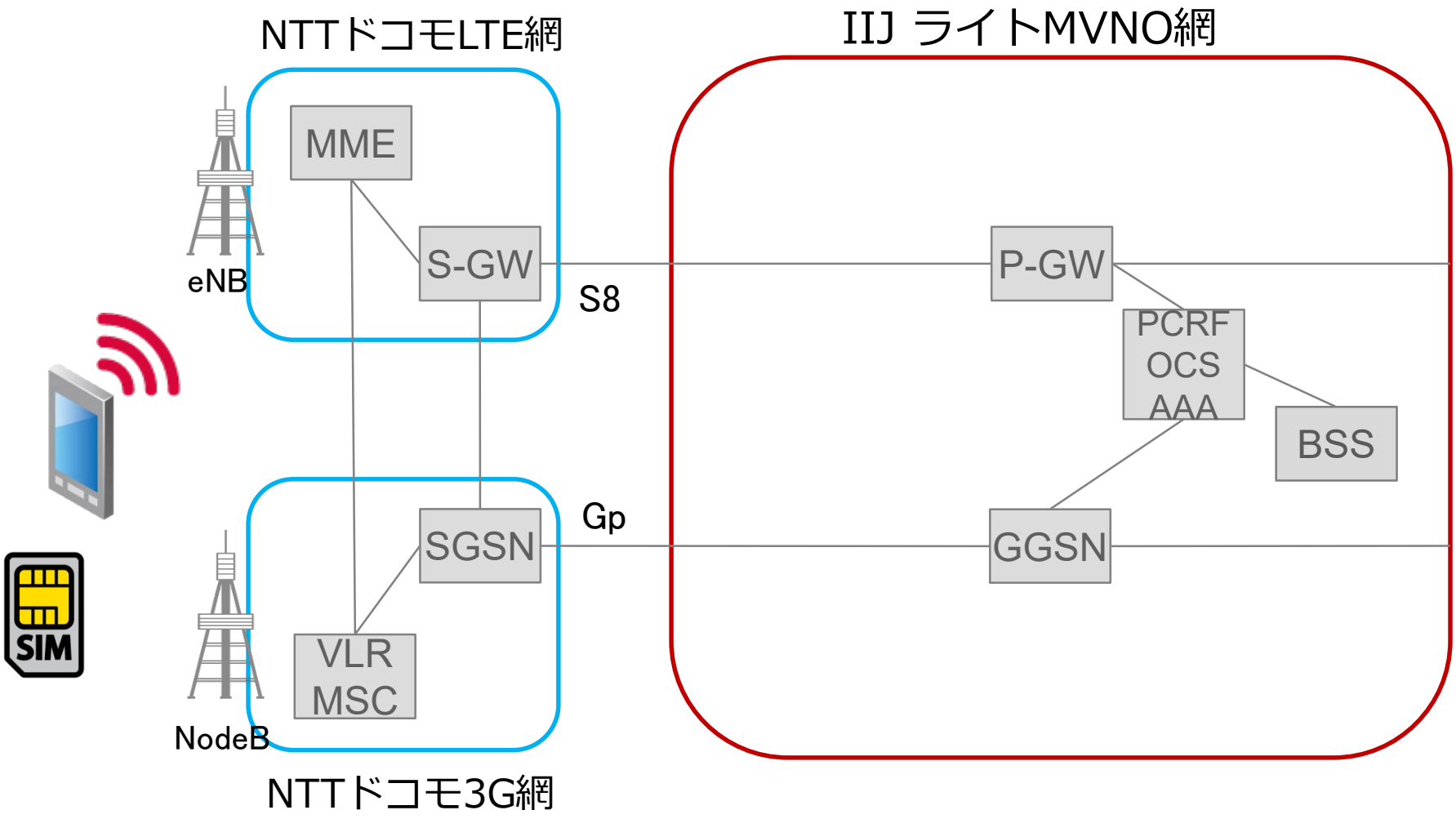
eSIM

- 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

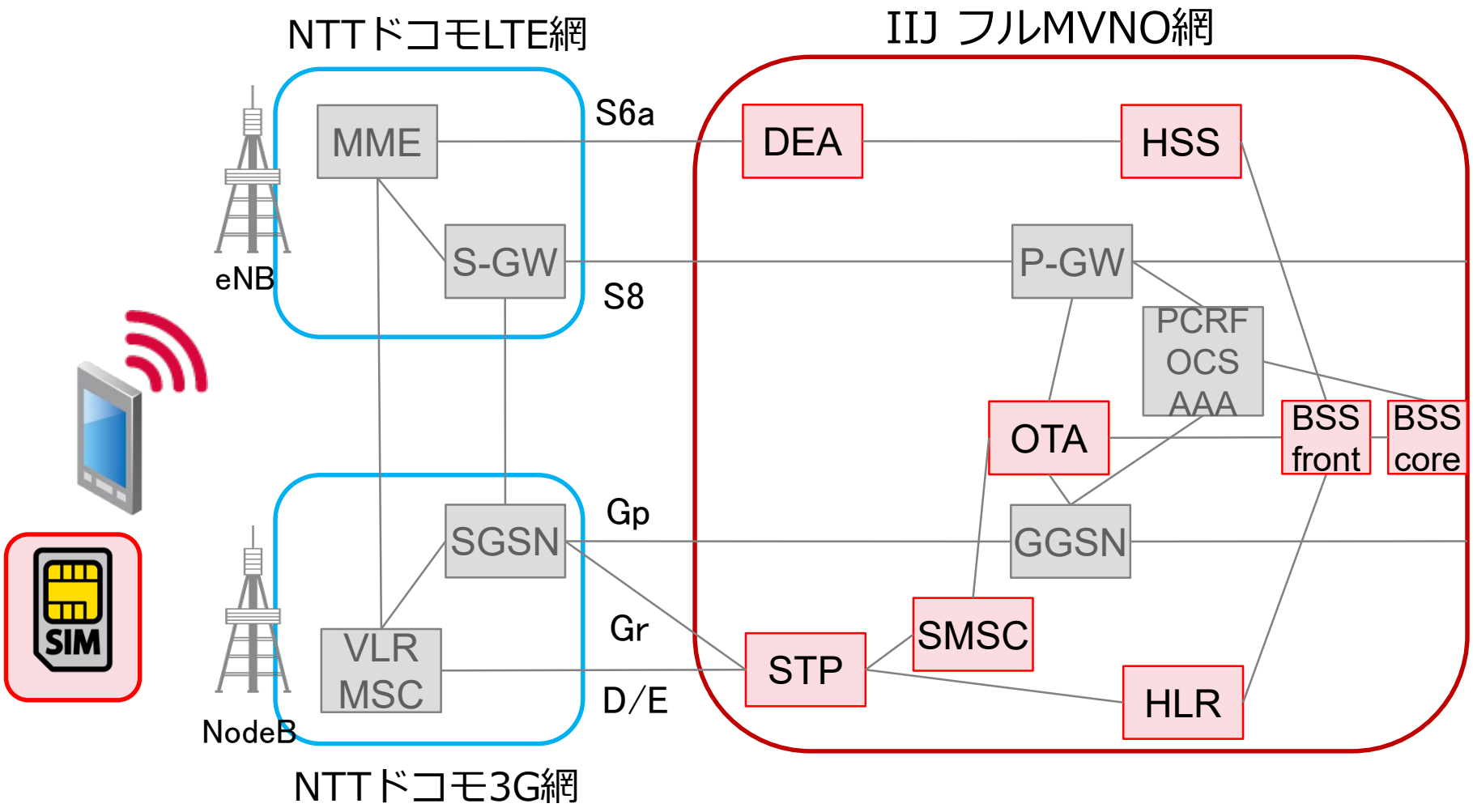
- IIJ MVNOインフラ概要
- IIJ フルMVNOサービス領域
- eSIMとは？
- IIJ PoCについて
- eSIMの仕組みについて
- まとめ

IIJ ライトMVNOインフラ概要



いわゆるL2接続

IIJ フルMVNOインフラ概要

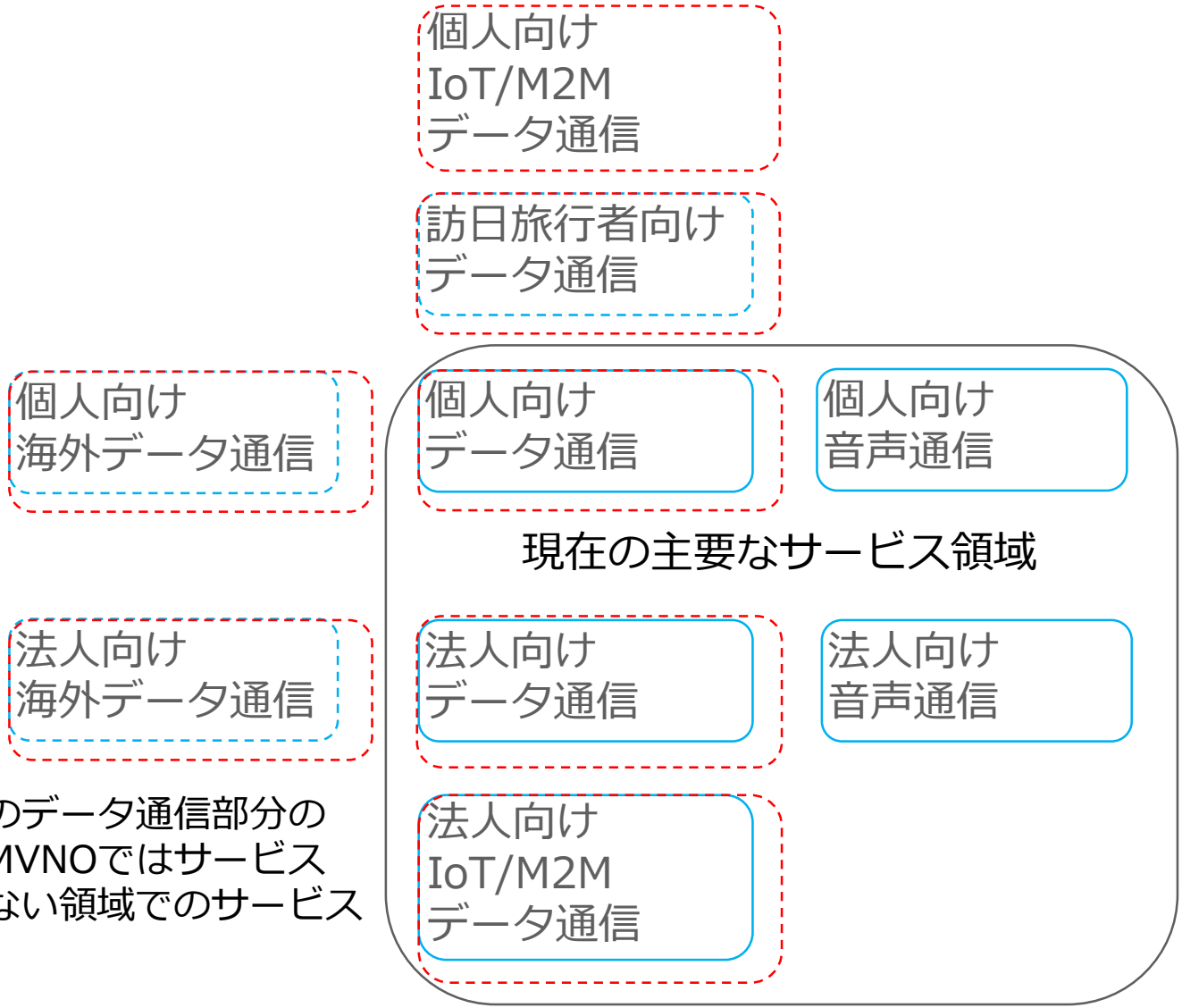


加入者管理関連/OTA機能/IIJ独自SIMの開発

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



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
IoT/M2M
データ通信

IIJmio　IoTサービス
(８月開始)

訪日旅行者向け
データ通信

Japan Travel SIM
(4月開始)

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

コンシューマ規格に
基づくeSIMサービス
(開発着手)

法人向け
海外データ通信

法人向け
データ通信

音声通信

ライフサイクル管理
(3月開始)

国際ローミングオプション
(7月開始)

法人向け
IoT/M2M
データ通信

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

SIMalliance eUICC Profile Package: Interoperable Format Technical Specification

SGP.21より引用

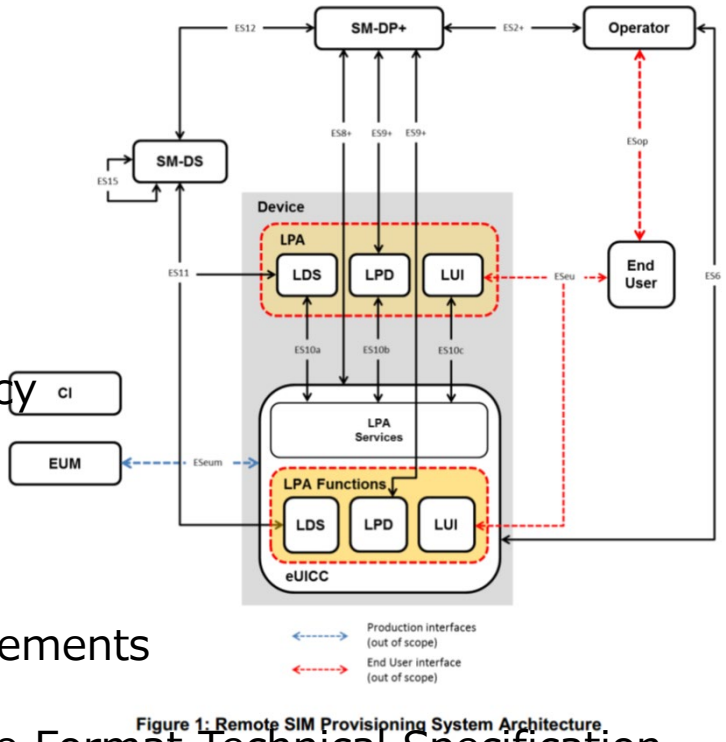


Figure 1: Remote SIM Provisioning System Architecture

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

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

SGP.21より引用

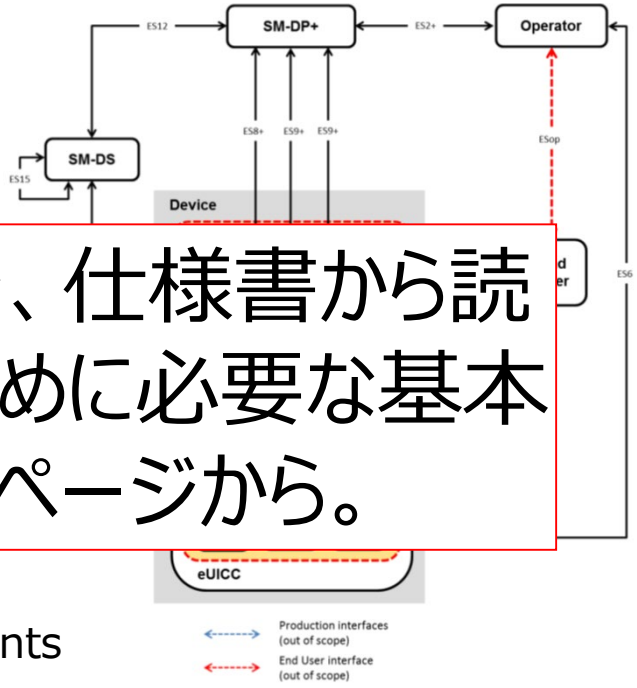


Figure 1: Remote SIM Provisioning System Architecture

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ー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) 44003xxxxxxxxx

Ki: 認証鍵
パスワード相当

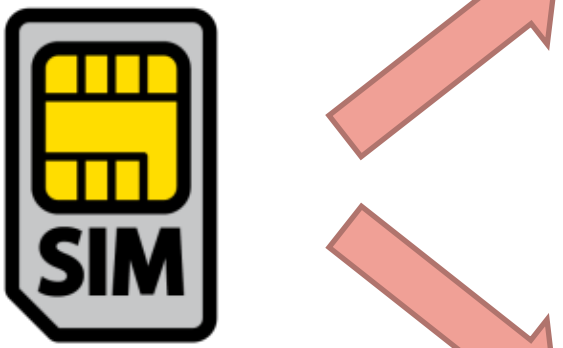
その他: 端末挙動を制御する値
独自のJavaプログラムも動作

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



SIM プロファイル

SIM構成データ
- IMSI
- 認証鍵

.
.

eUICCカード/チップ
- 耐タンパ性を持つHW
- SIMプロファイルを読み込んでSIMとして動作

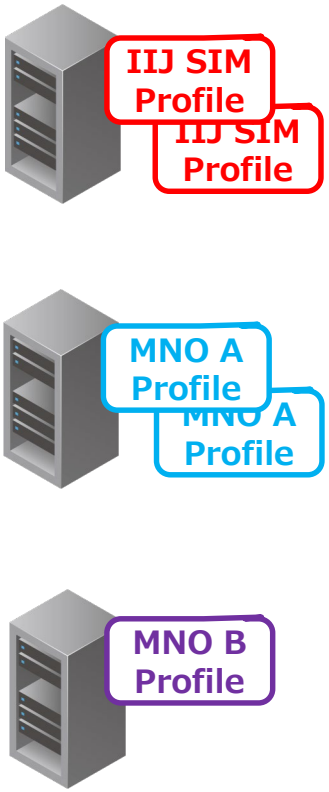
eSIMとは？ - 5

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

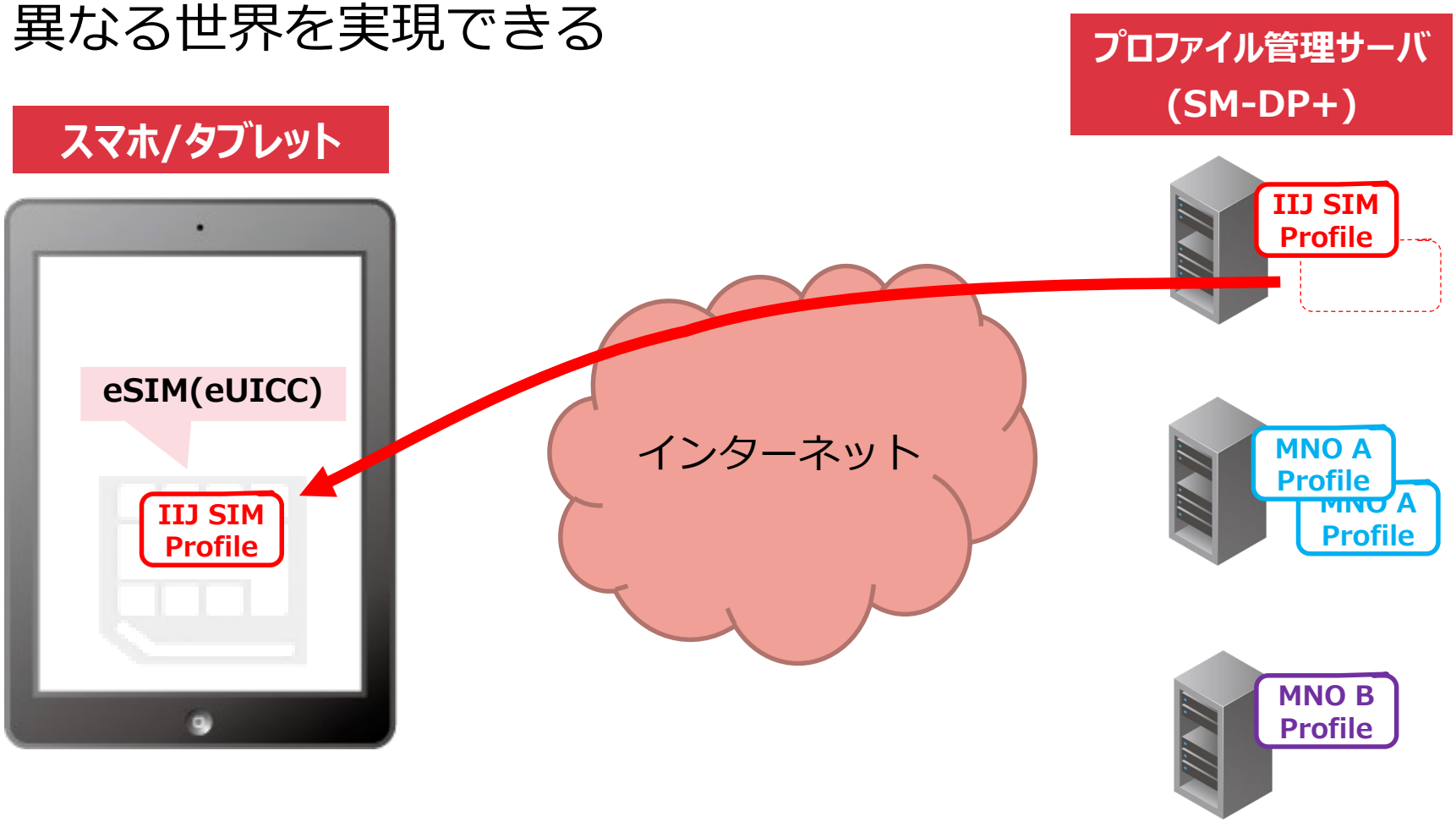
インターネット

プロファイル管理サーバ
(SM-DP+)



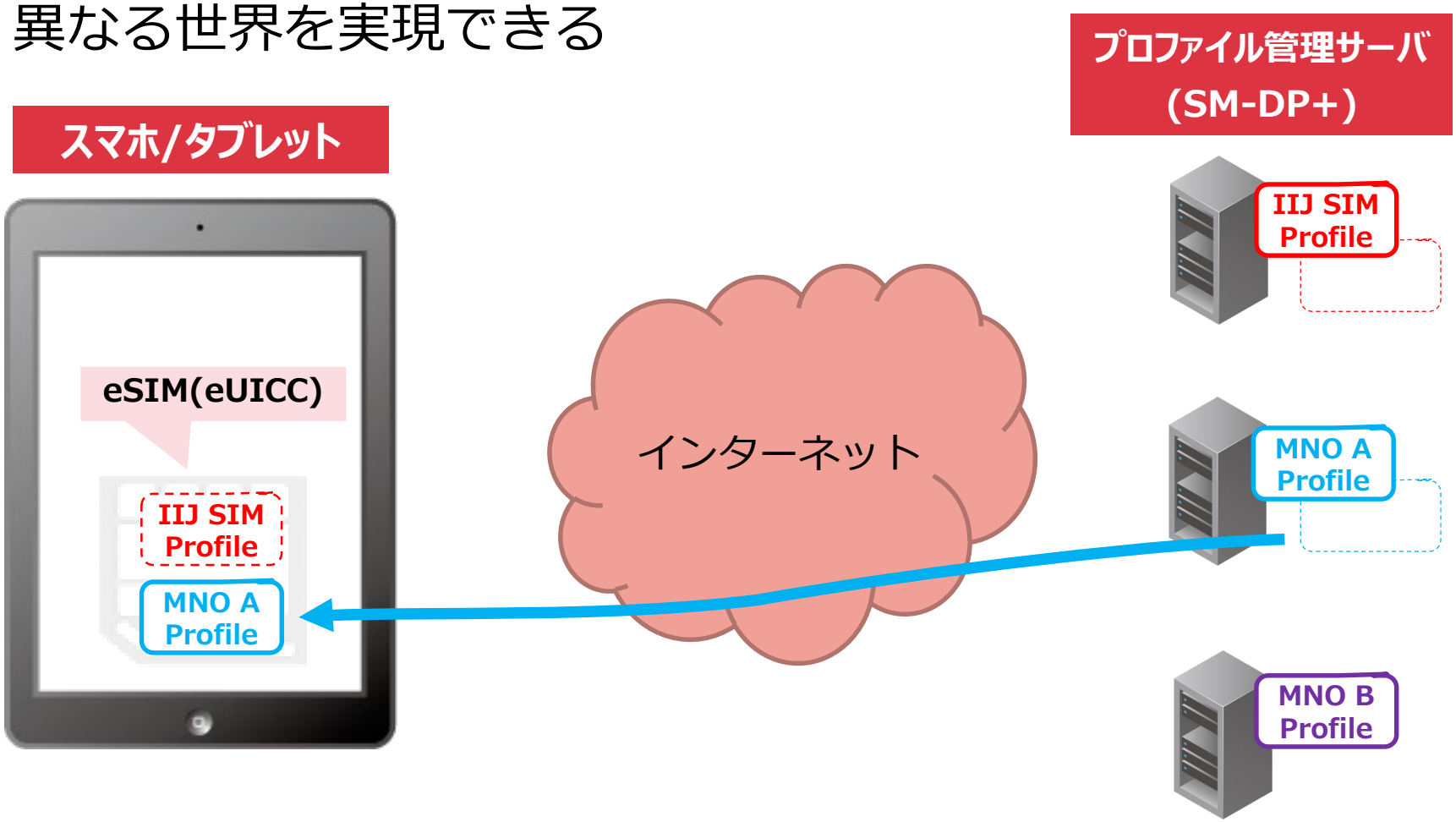
eSIMとは？ - 6

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

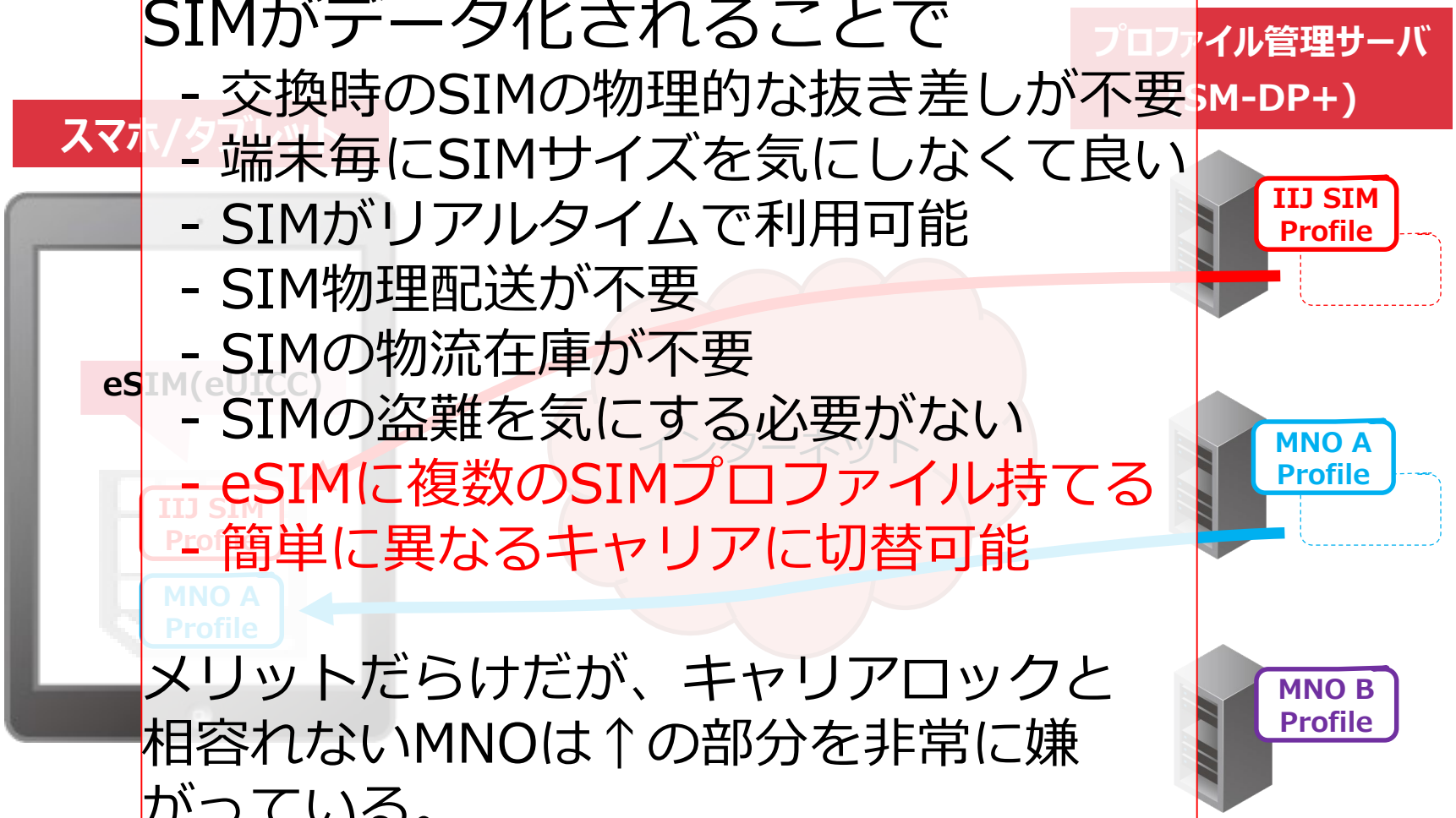
SIMのハードとデータを分離することで今までとは
異なる世界を実現できる



eSIMとは？ - 8

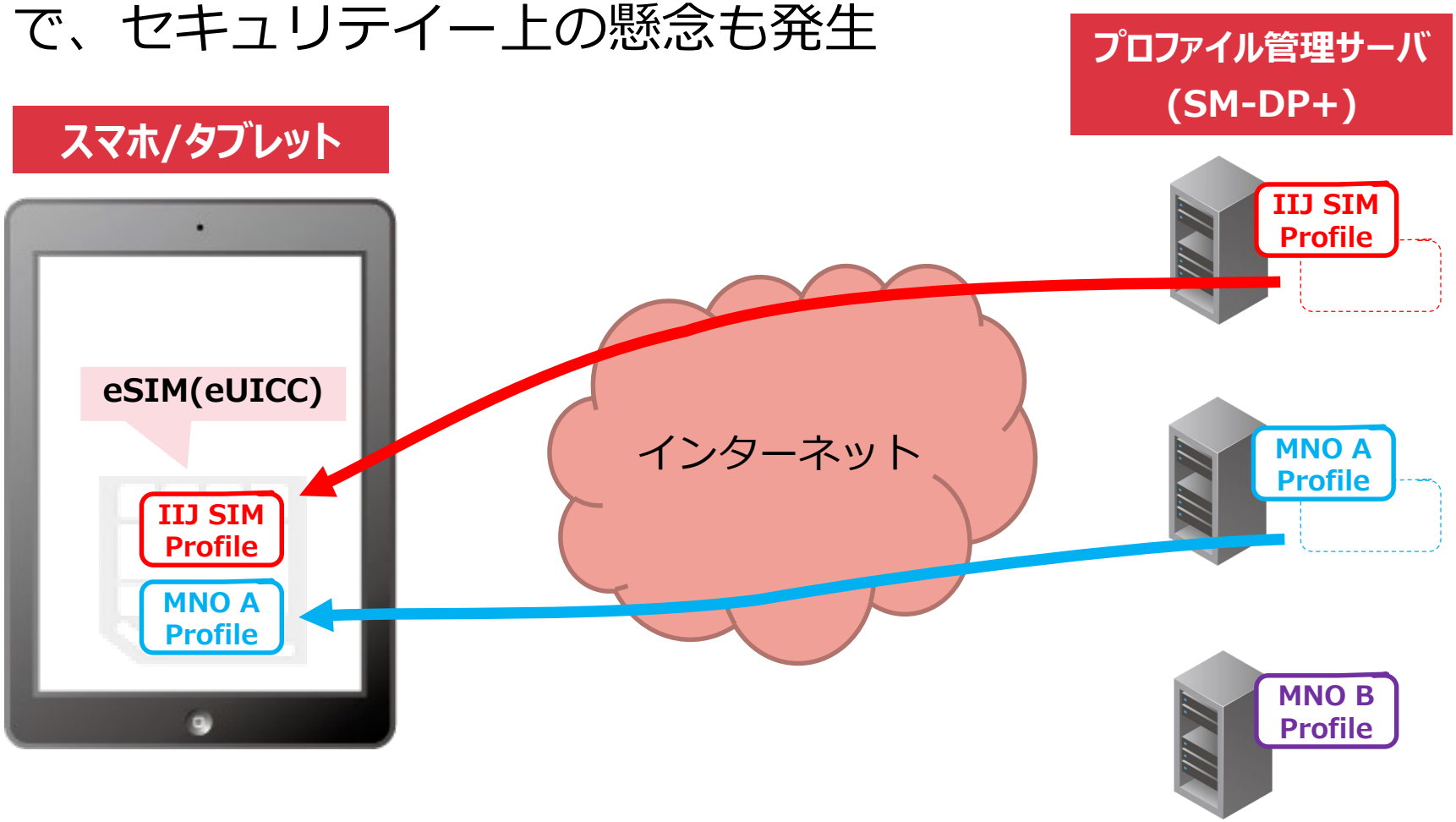
SIMがデータ化されることで
- 交換時のSIMの物理的な抜き差しが不要
- 端末毎にSIMサイズを気にしなくて良い
- SIMがリアルタイムで利用可能
- SIM物理配送が不要
- SIMの物流在庫が不要
- SIMの盗難を気にする必要がない
- eSIMに複数のSIMプロファイル持てる
- 簡単に異なるキャリアに切替可能

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。

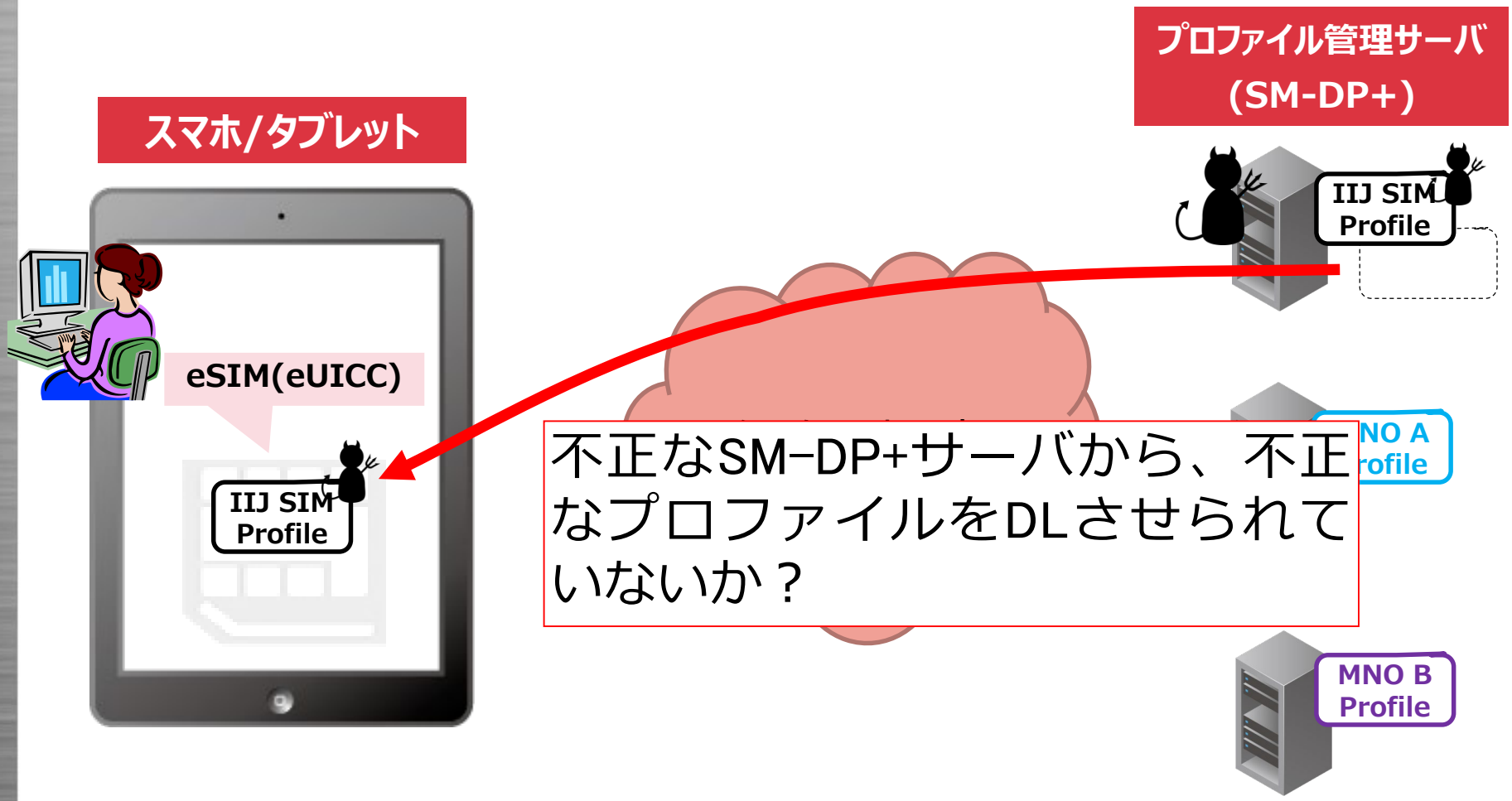


eSIMとは？ - 9

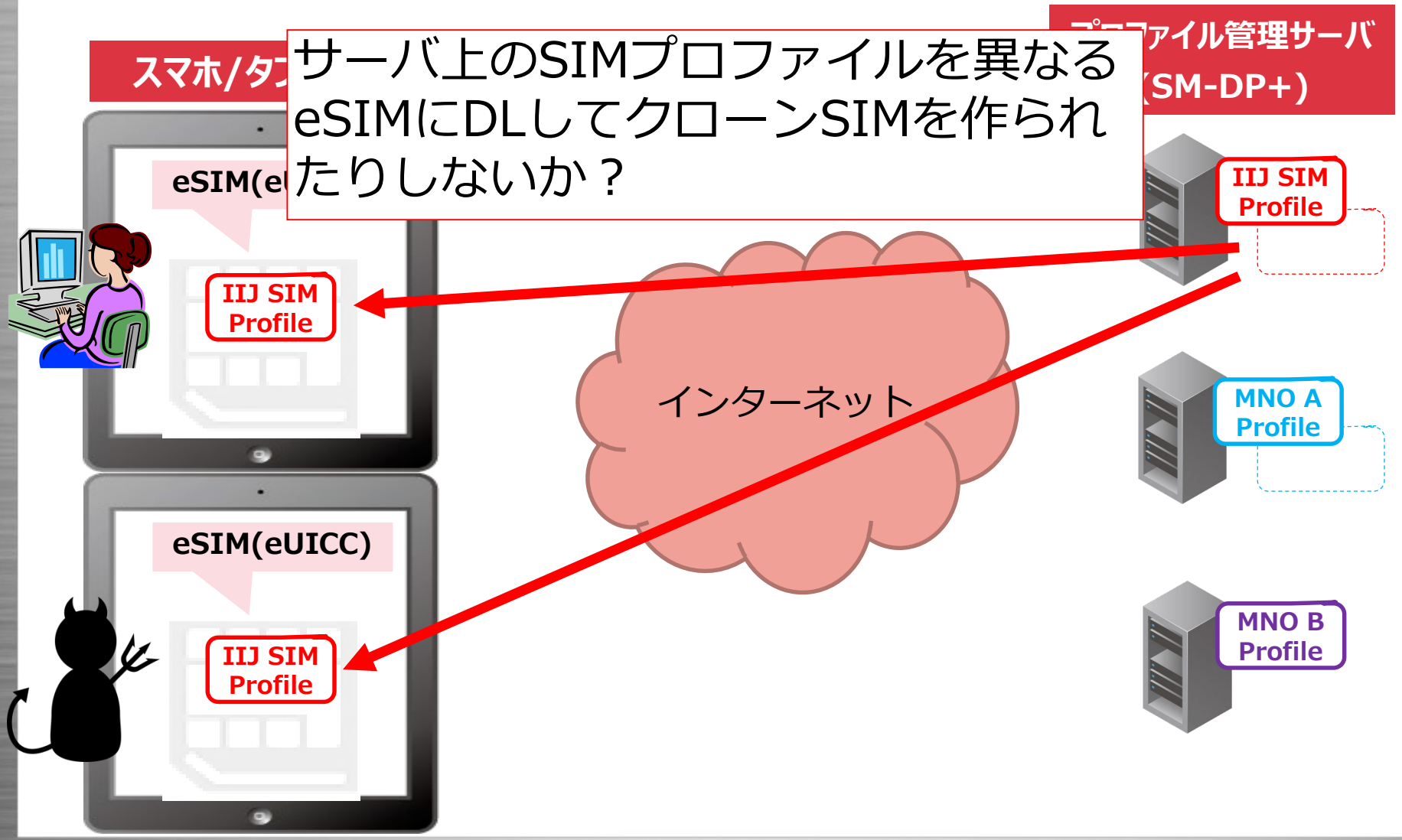
SIMのデータ化やリモートサーバからDLを可能にしたことで、セキュリテイー上の懸念も発生



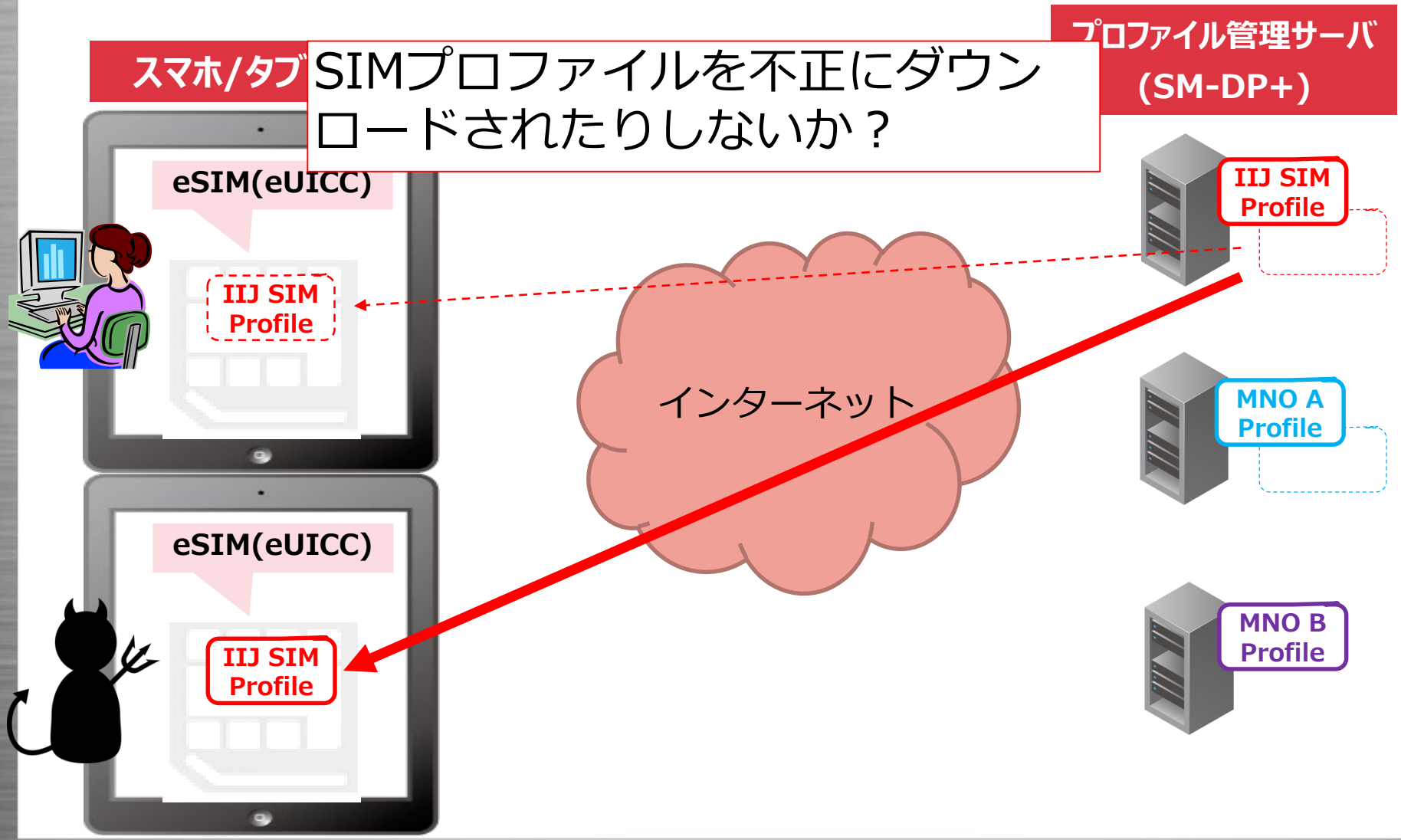
eSIMとは？ - 10


スマホ/タブレット
プロファイル管理サーバ
(SM-DP+)
eSIM(eUICC)
IIJ SIM
Profile
IIJ SIM
Profile
NO A
rofile
MNO B
Profile
不正なSM-DP+サーバから、不正なプロファイルをDLさせられていないか？

eSIMとは？ - 11

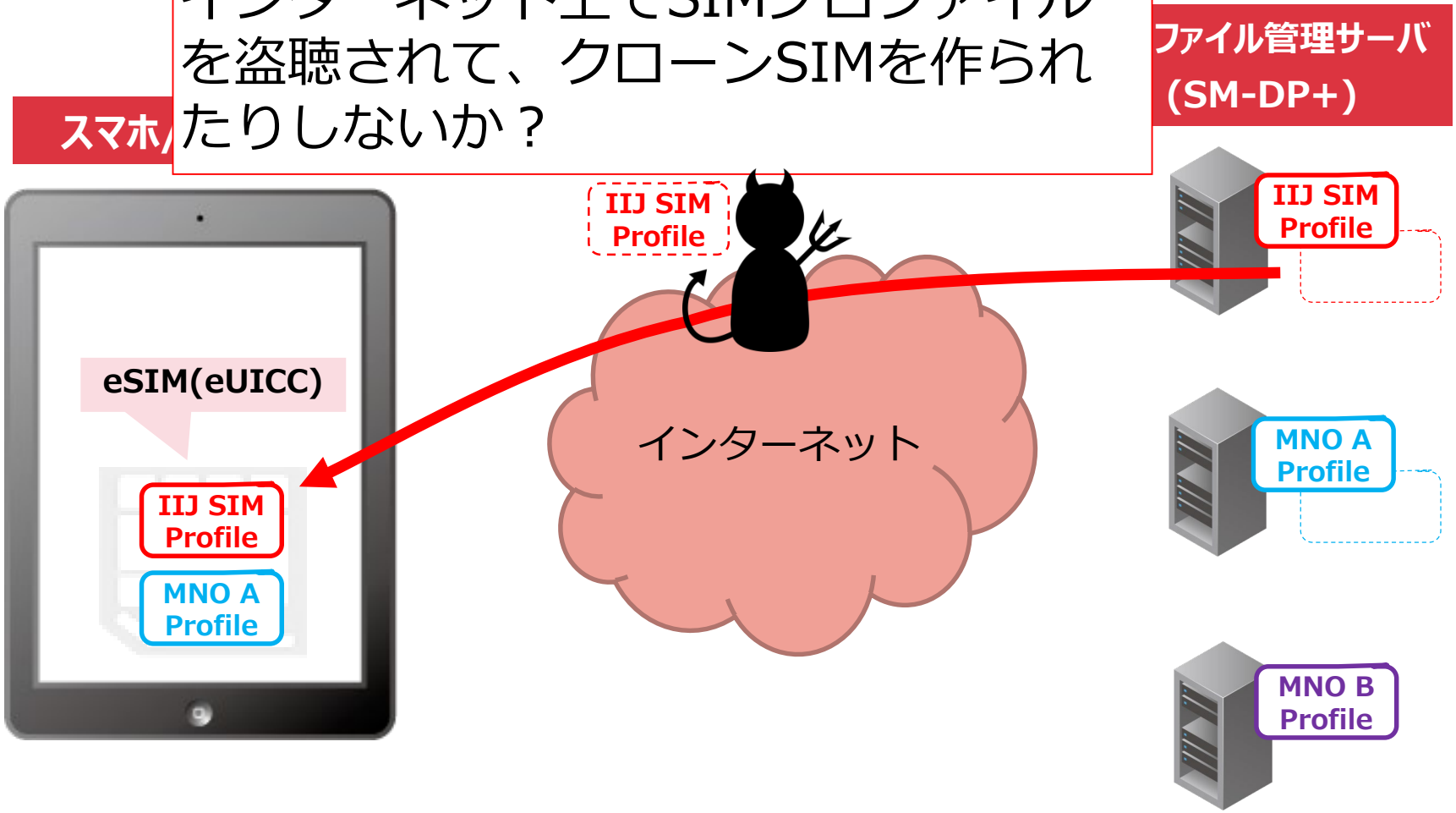


eSIMとは？ - 12



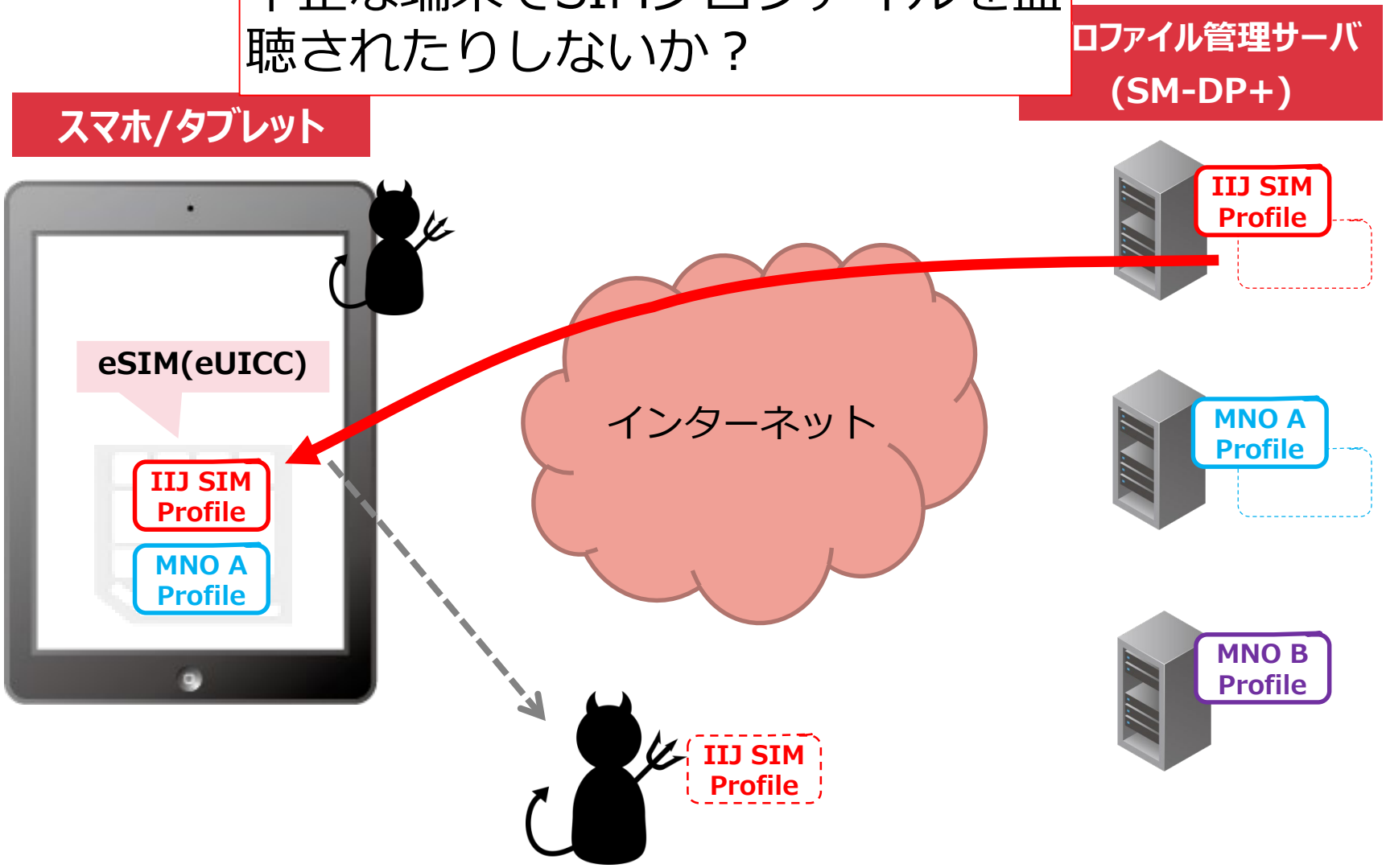
eSIMとは？ - 13

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？



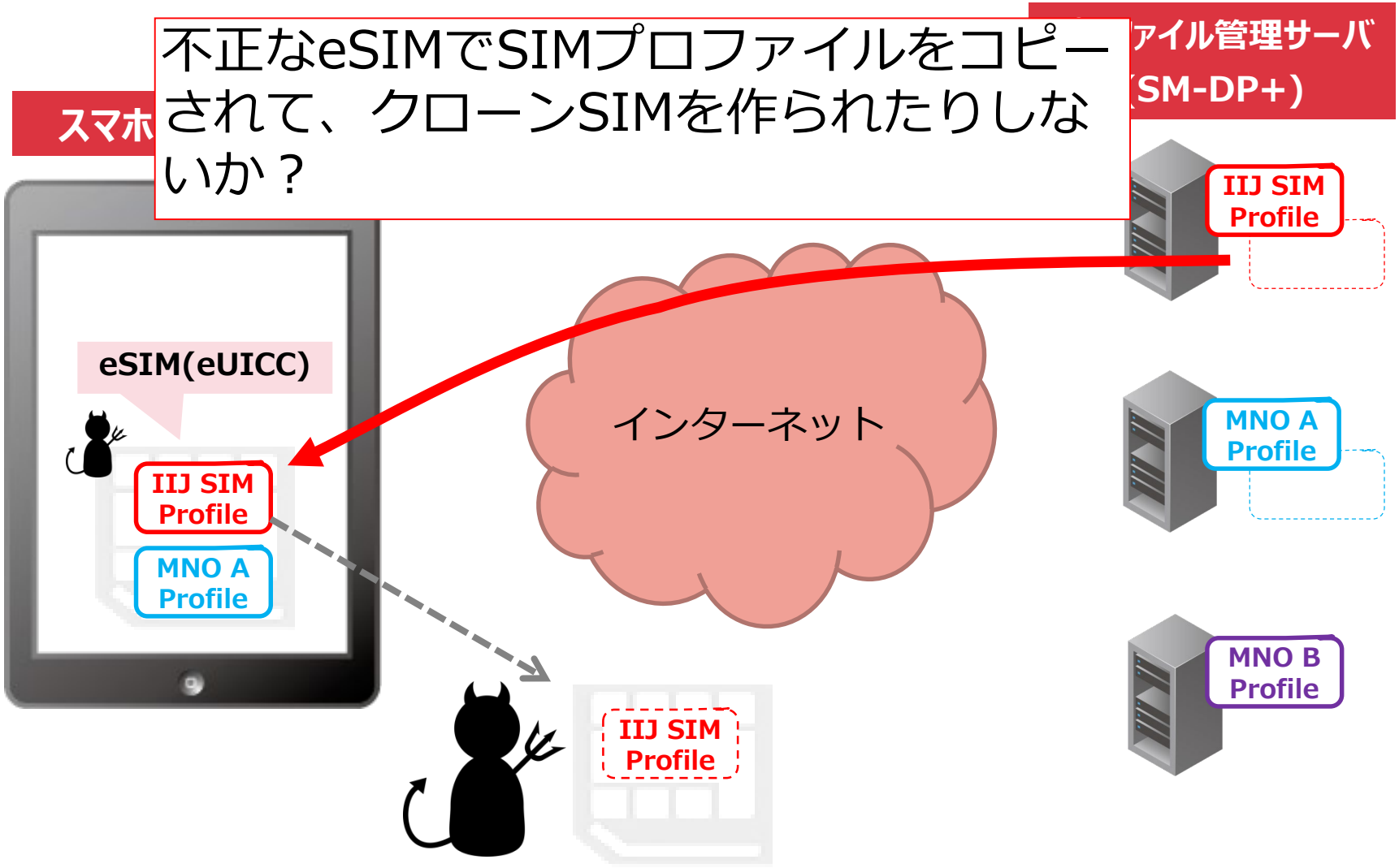
eSIMとは？ - 14

不正な端末でSIMプロファイルを盗聴されたりしないか？



eSIMとは？ - 15

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？



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

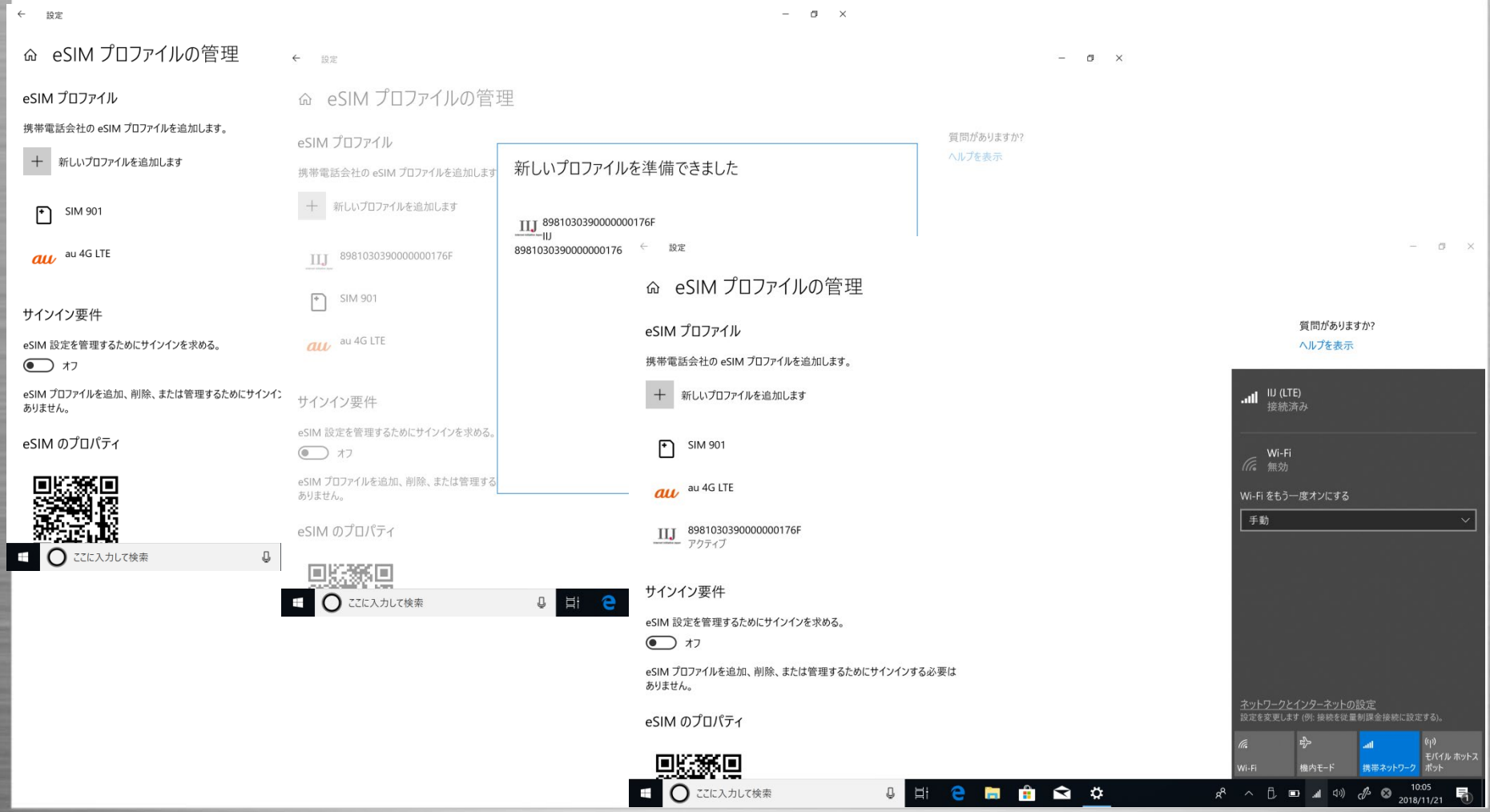
- PoC内容
  - IIJ SIMプロファイルをダウンロードして、商用網に接続可能かの確認
  - eSIM対応デバイスでの動作確認
    - Microsoft Surface Pro LTE Advanced
    - Windows PC(V社,H社)
    - Apple(iOS 12.1以降)
      - iPhone XS/XR, iPad Pro(2018年)
    - eSIM内蔵Android端末(デバイス名非公開)
  - 主要SIMサプライヤーからeSIMカードを調達し動作確認

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.iij.ad.jp/news/pressrelease/2018/0712.html



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)

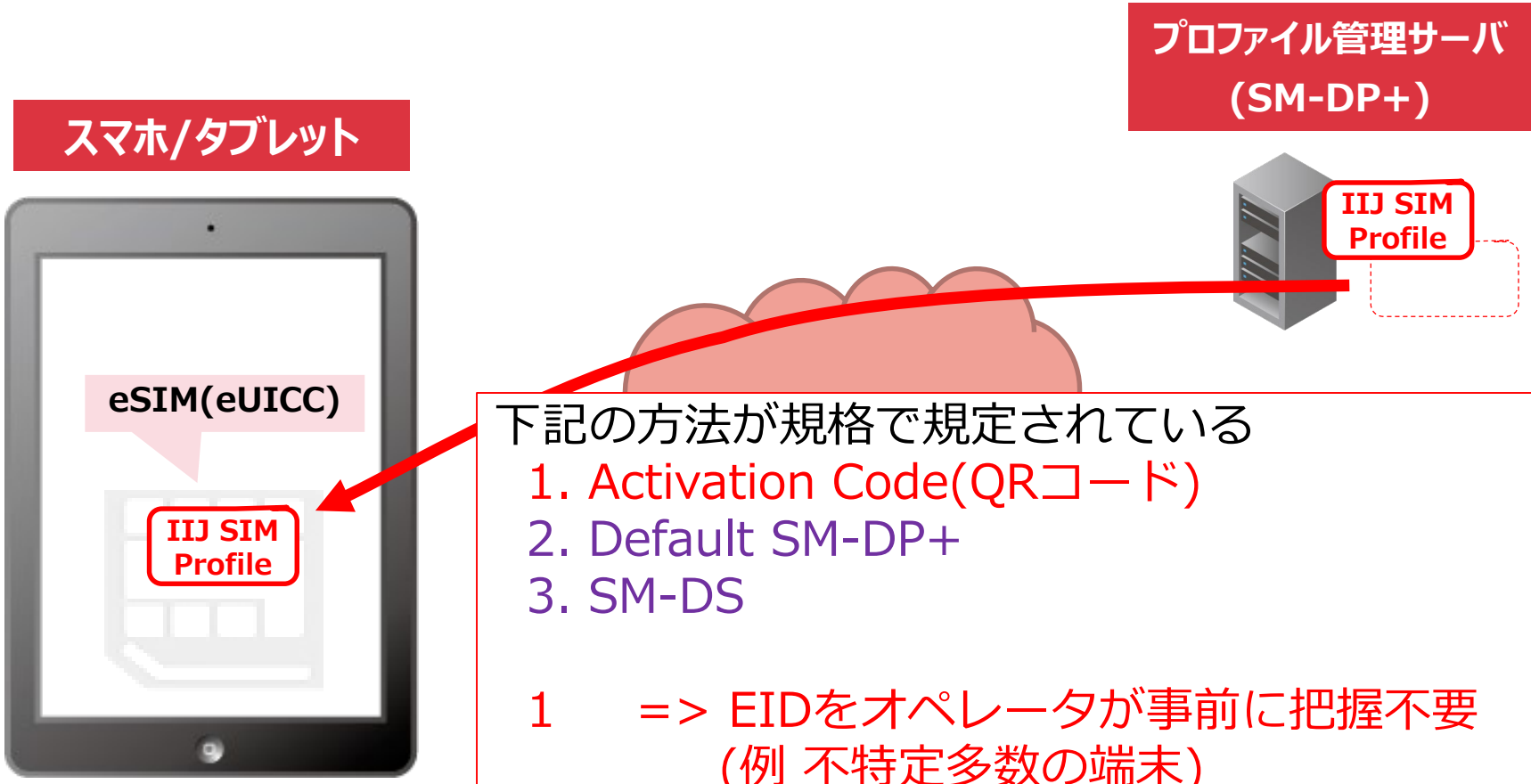
eSIMについて

- 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
  (if SM-DP+ OID is not present and Confirmation Code Required Flag is present)

  ←→ Confirmationコードを必要とするか
- 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
  (If SM-DP+ OID is present, Activation token is left blank and Confirmation Code Required Flag is not present)

  ←→ サーバの認証用証明書(Cert.DPauth.DCDSA)のOID

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

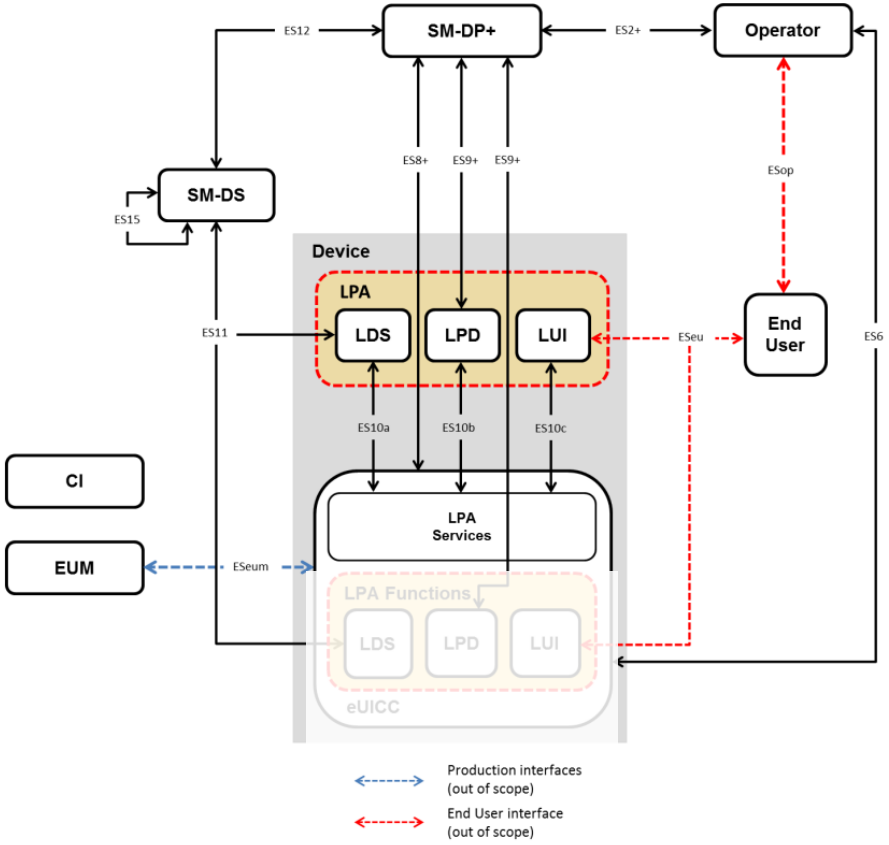
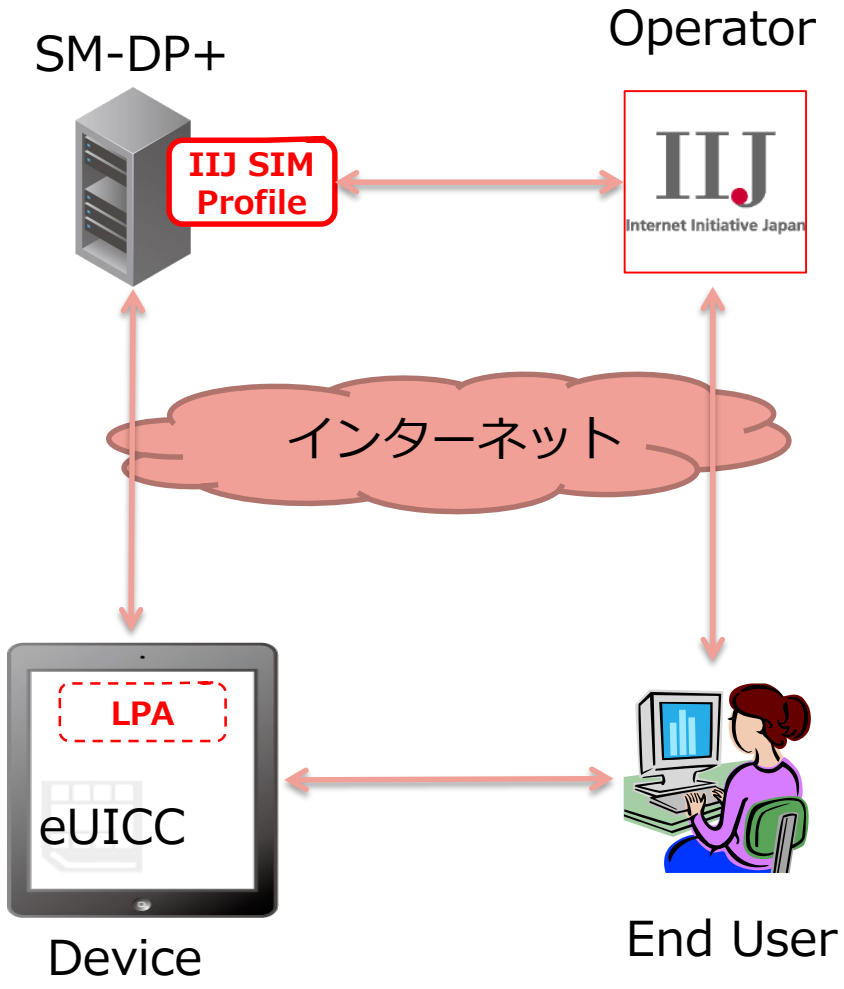


Figure 1: Remote SIM Provisioning System Architecture

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)

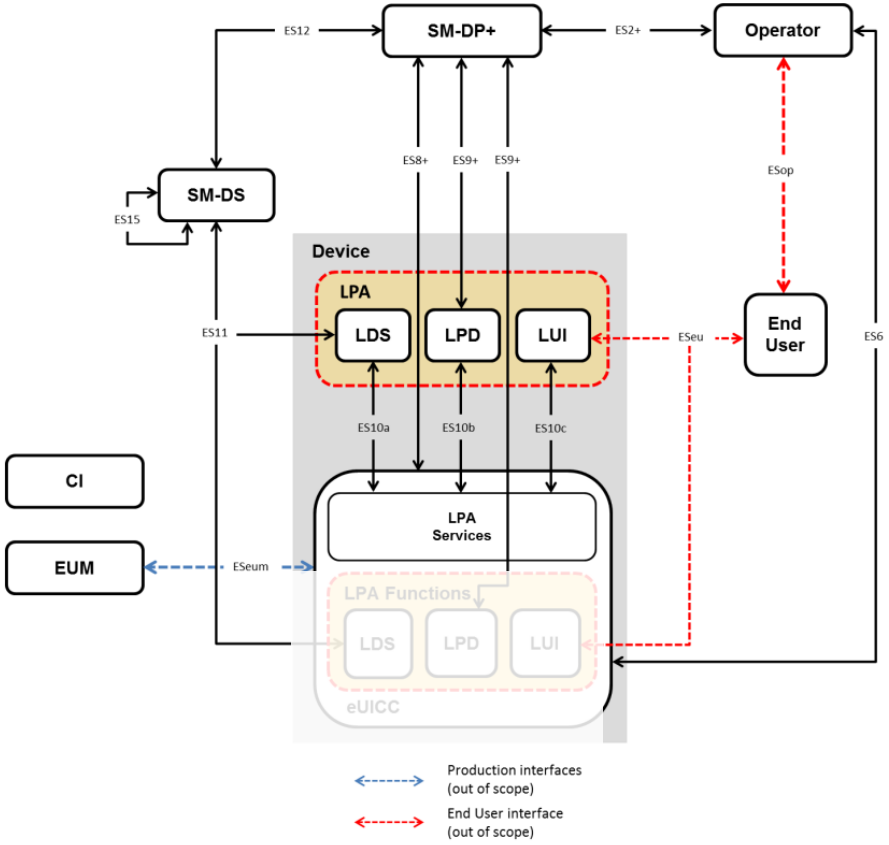


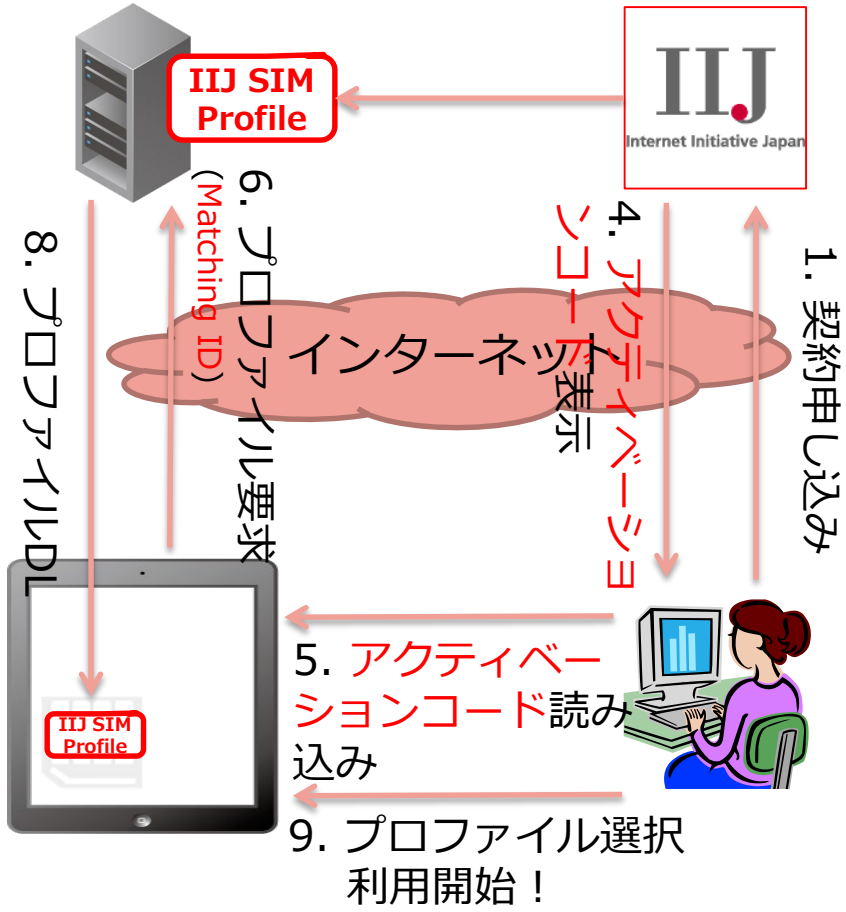
Figure 1: Remote SIM Provisioning System Architecture

SGP.21より引用

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



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)

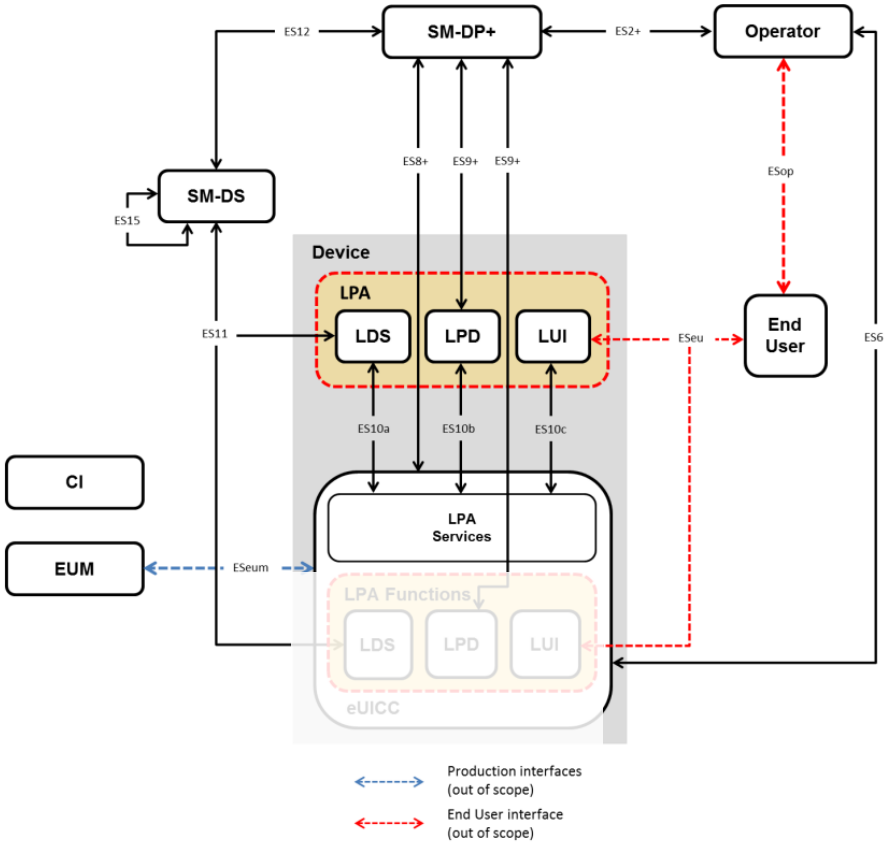
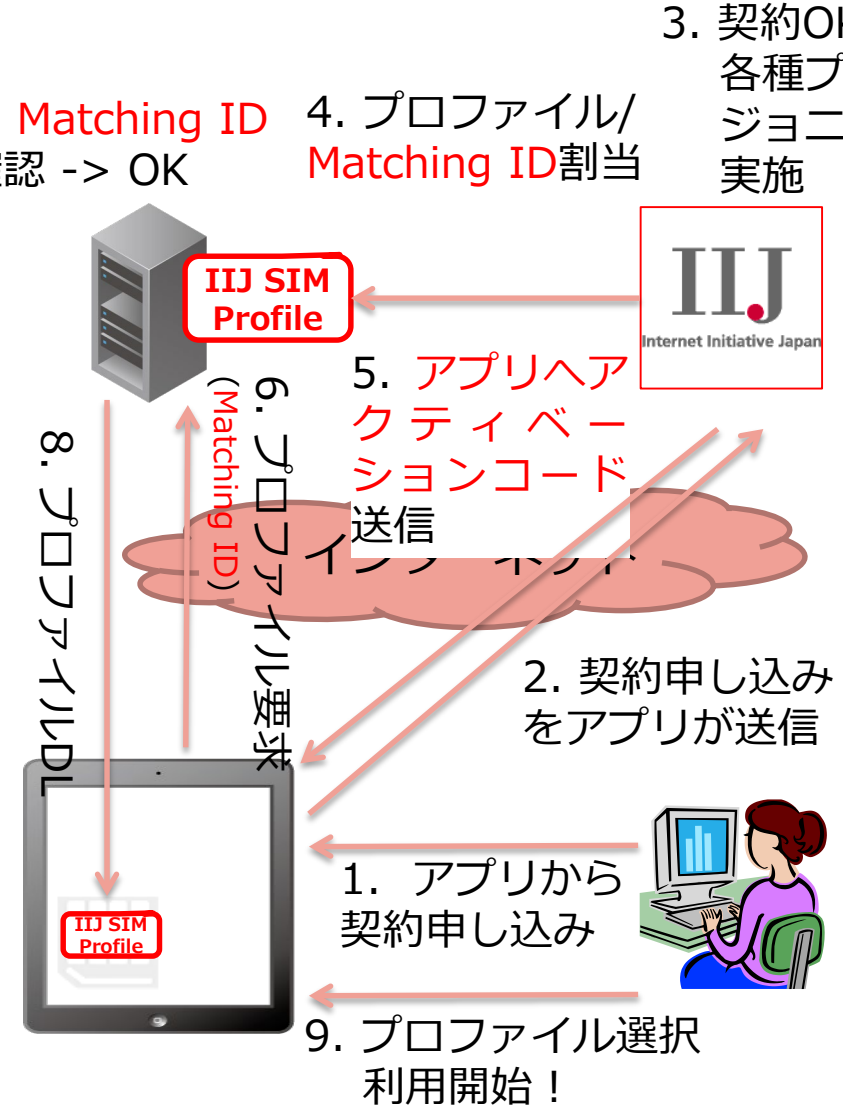


Figure 1: Remote SIM Provisioning System Architecture

SGP.21より引用



プロファイルのダウンロード方法 - 6

2. Default SM-DP+

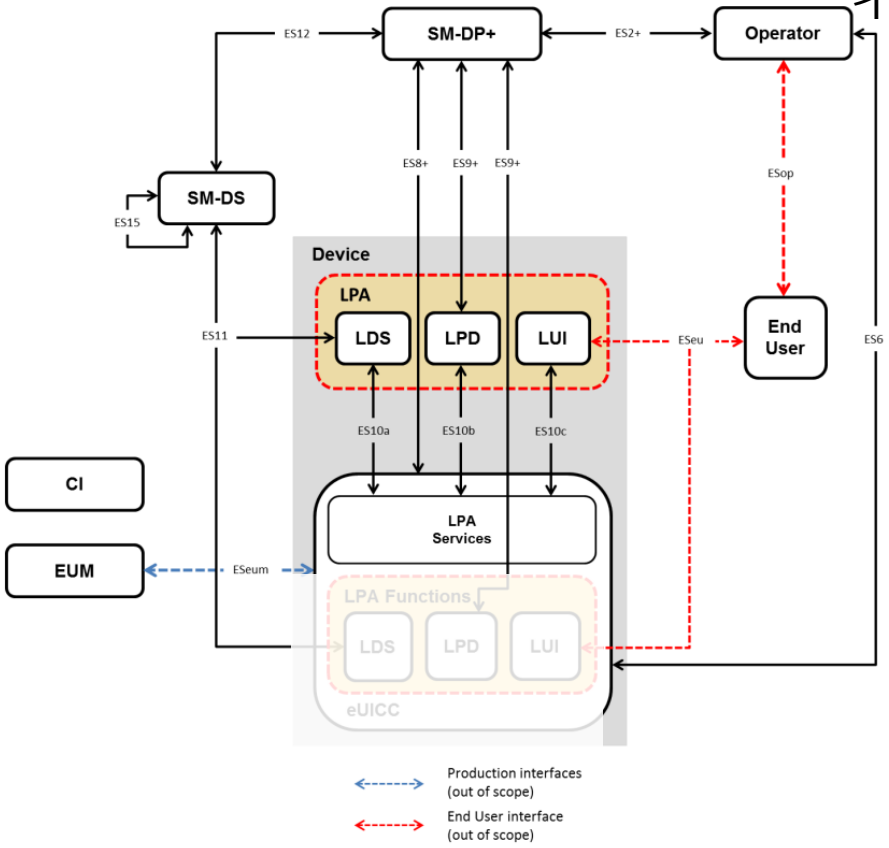
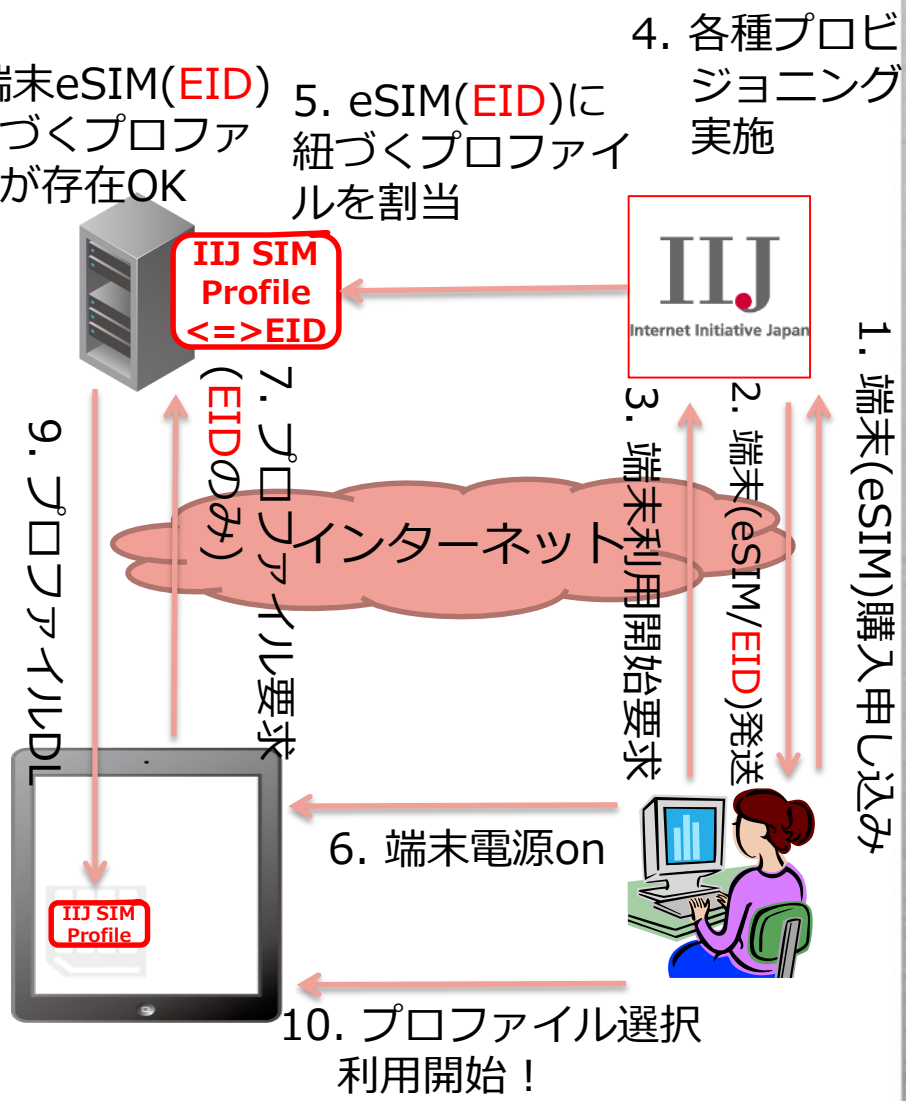


Figure 1: Remote SIM Provisioning System Architecture

SGP.21より引用



プロファイルのダウンロード方法 - 7

3. SM-DS

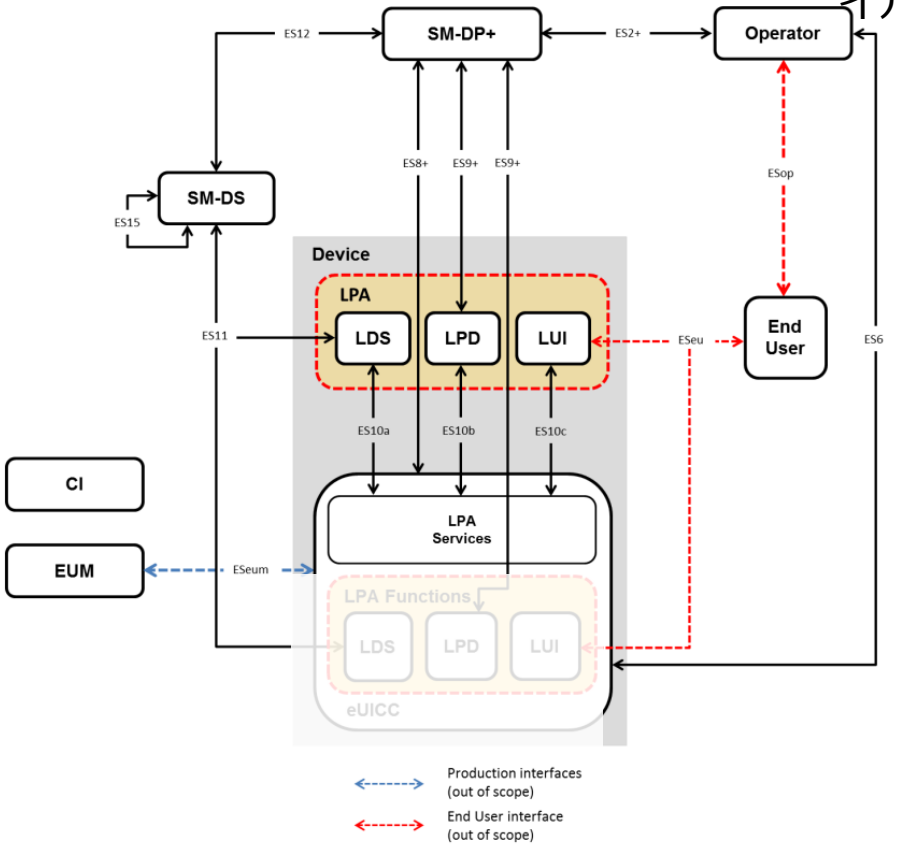
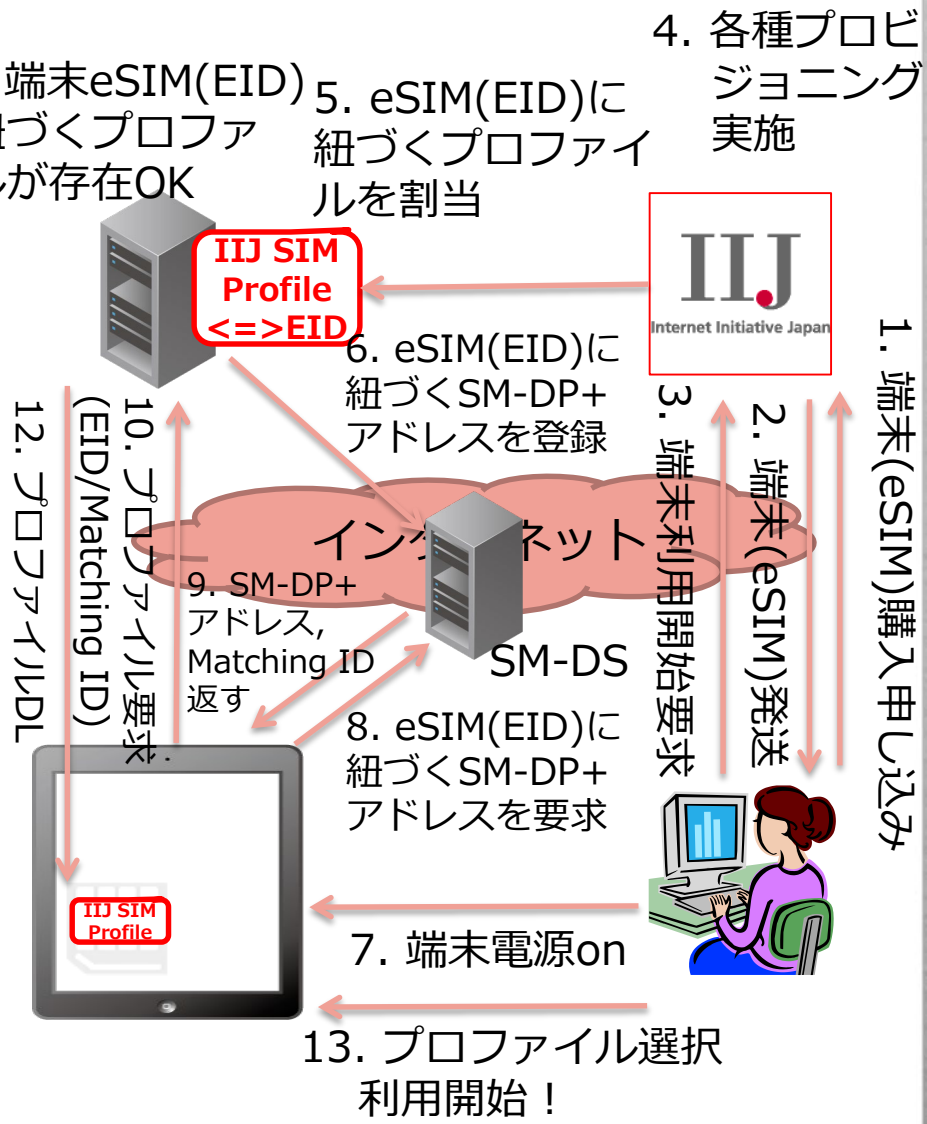


Figure 1: Remote SIM Provisioning System Architecture

SGP.21より引用



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プロファイルとは - 1

- eUICC HW実装に依存せず、SIMが持つ機能、ファイル/認証/セキュリティー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る
    - 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プロファイルとは - 2

- SIMプロファイ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	
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

IMSIなどを含む
ディレクトリの記述

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プロファイルとは - 3

- SIMプロファイルの具体例について – Profile HEADER

11.2.2 Profile HEADER

ASN.1 Format	DER TLV encoding

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
  }
}
	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

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

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 : {
	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

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

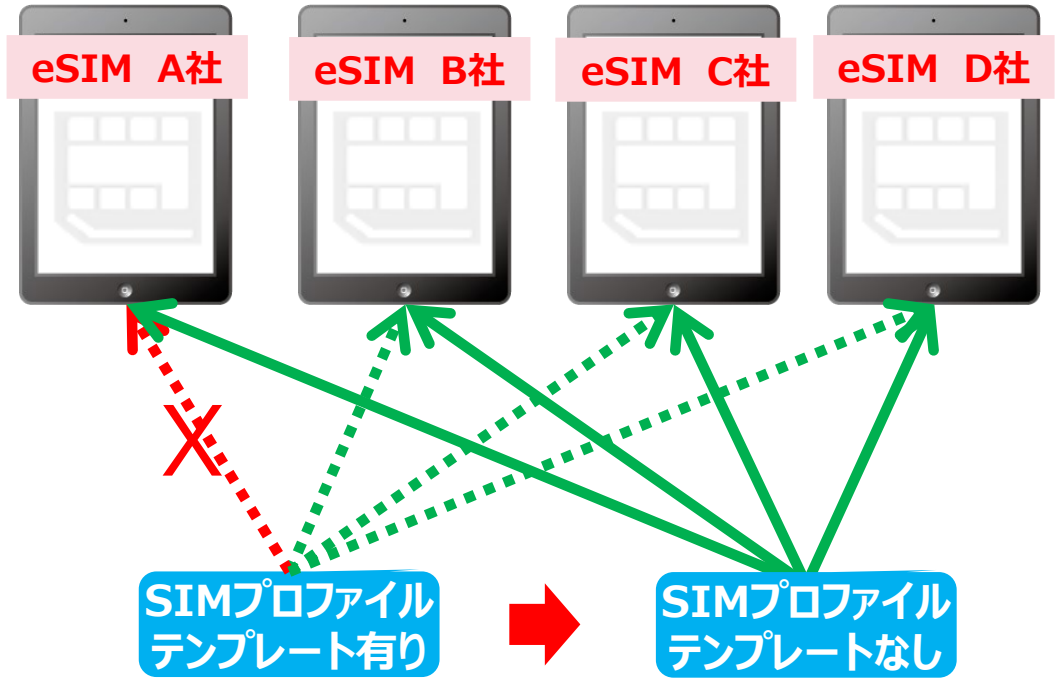
usimValue ProfileElement ::= usim : {
  usim-header {
  mandated NULL,
  identification 4
  },
  templateID { 2 23 143 1 2 4 },
  adf-usim {
  fileDescriptor : {
  fileID '7FF1'H,
  dfName 'A0000000871002FF33FF018900000100'H,
  pinStatusTemplateDO '01810A'H
  }
  },
	B3 77
	  A0 05
	  80 00
	  81 01 04
	
	  81 06 67810F010204
	  A2 1D
	  A1 1B
	  83 02 7FF1
	  84 10 A0000000871002FF33FF018900000100
	  C6 03 01810A

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
  },
	A3 0B
	
	  83 09 082943019134876765
	
	  A4 06
	  A1 04
	  C7 02 2F06
	
	  A8 0F
	
	  83 0D 0A2E178CE73204000000000000
	
	  AD 0E
	  83 0C 0253494D616C6C69616E6365

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

SIMプロファイルとは - 6

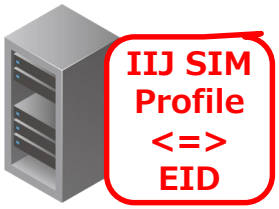
- 実証試験で遭遇した問題
  - eSIMベンダーが異なる場合に、プロファイルDLが失敗する場合があった
  - 標準化されているがプロファイルデータ解釈の互換性の問題があった
  - 商用展開前には、SIMプロファイルが各社のeSIMで動作するか十分な検証が必要



SIMプロファイルとは - 7

サーバ上の各プロファイルは状態を持って管理されている

プロファイル管理サーバ
(SM-DP+)



重複ダウンロードを防ぐために、各プロファイルは状態を持ち、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: - 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プロファイルとは - 8

サーバ上の各プロファイルは、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

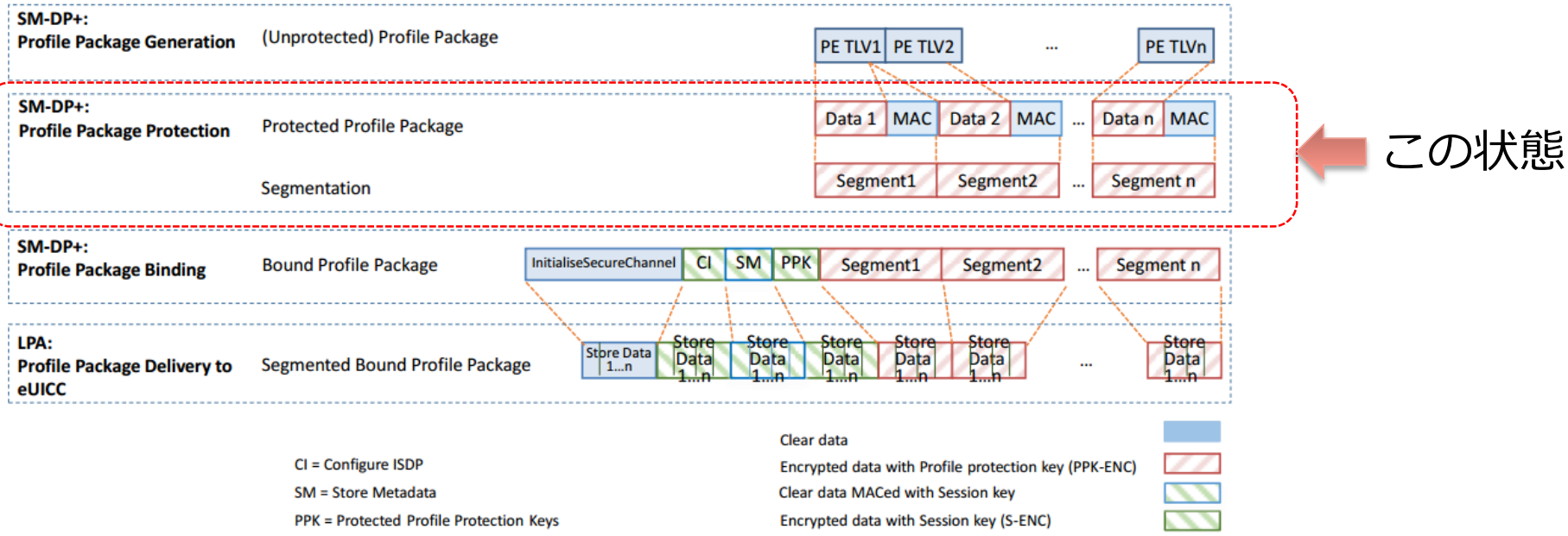


Figure 4: Profile Package stage Description

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

ICCID/IMSI
MSISDN等

SIM認証制御

OTA機能

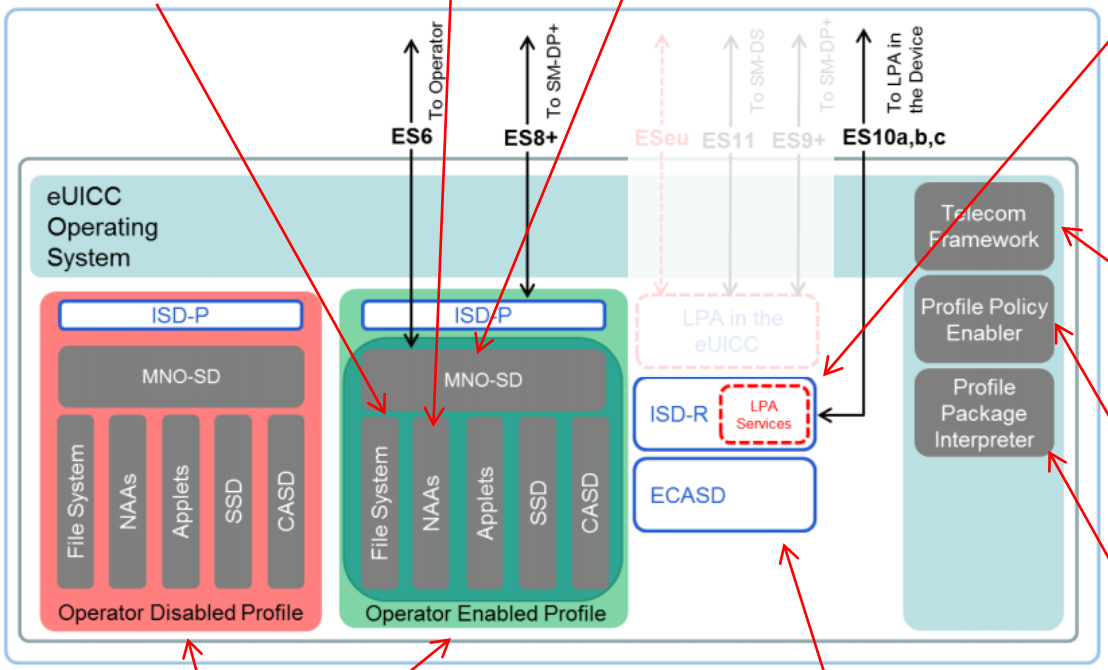


Figure 2: Schematic Representation of the eUICC
SGP.21より引用

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

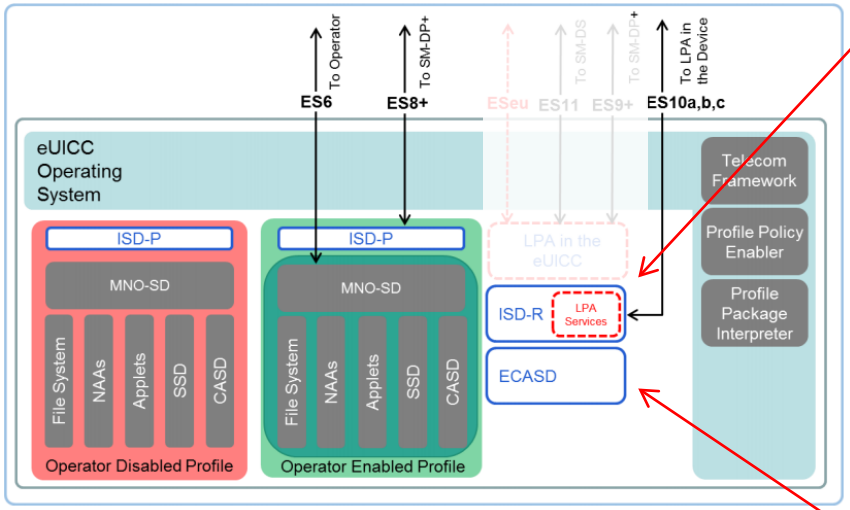


Figure 2: Schematic Representation of the eUICC

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

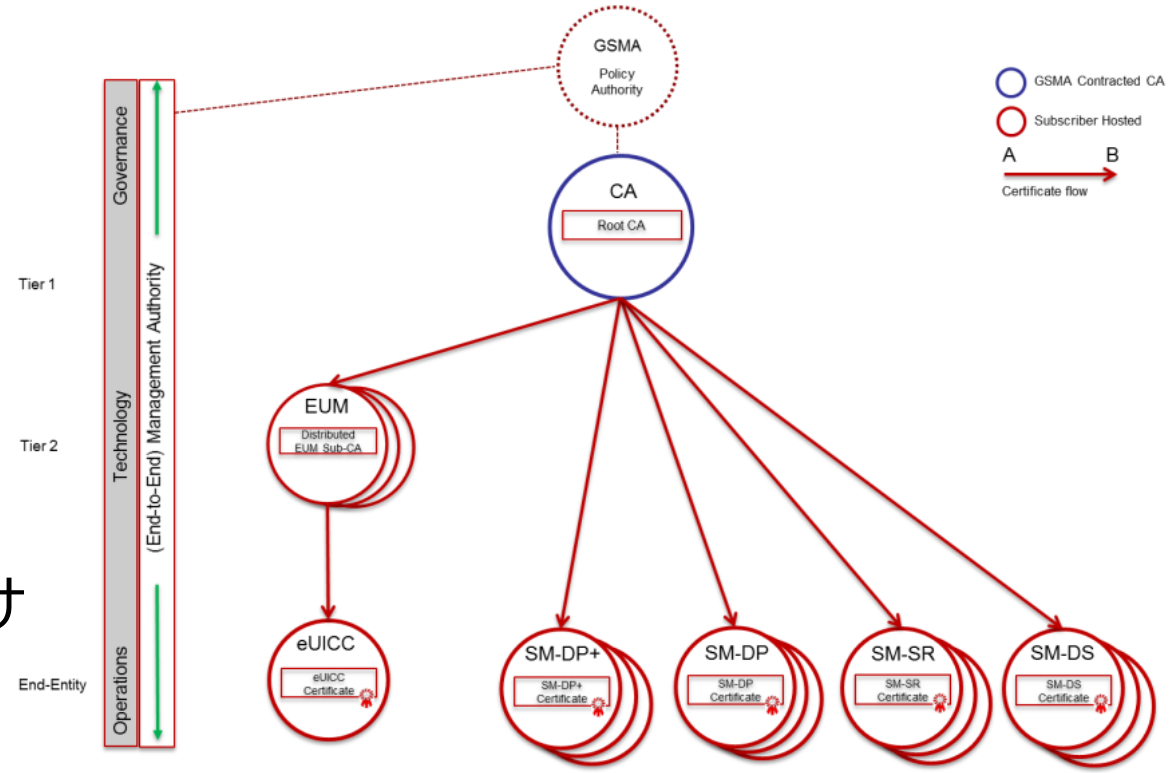
証明書/秘密鍵
- Root CI証明書
  - SM-DP+証明書の正当性確認
- EUM証明書(中間証明書)
- eUICC証明書, 秘密鍵
  - EID
  - eUICC自身の製造元とその正当性の証明
  - プロファイル暗号化等

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して貰う必要があるが、このためにはGSMAの認証を受ける必要がある

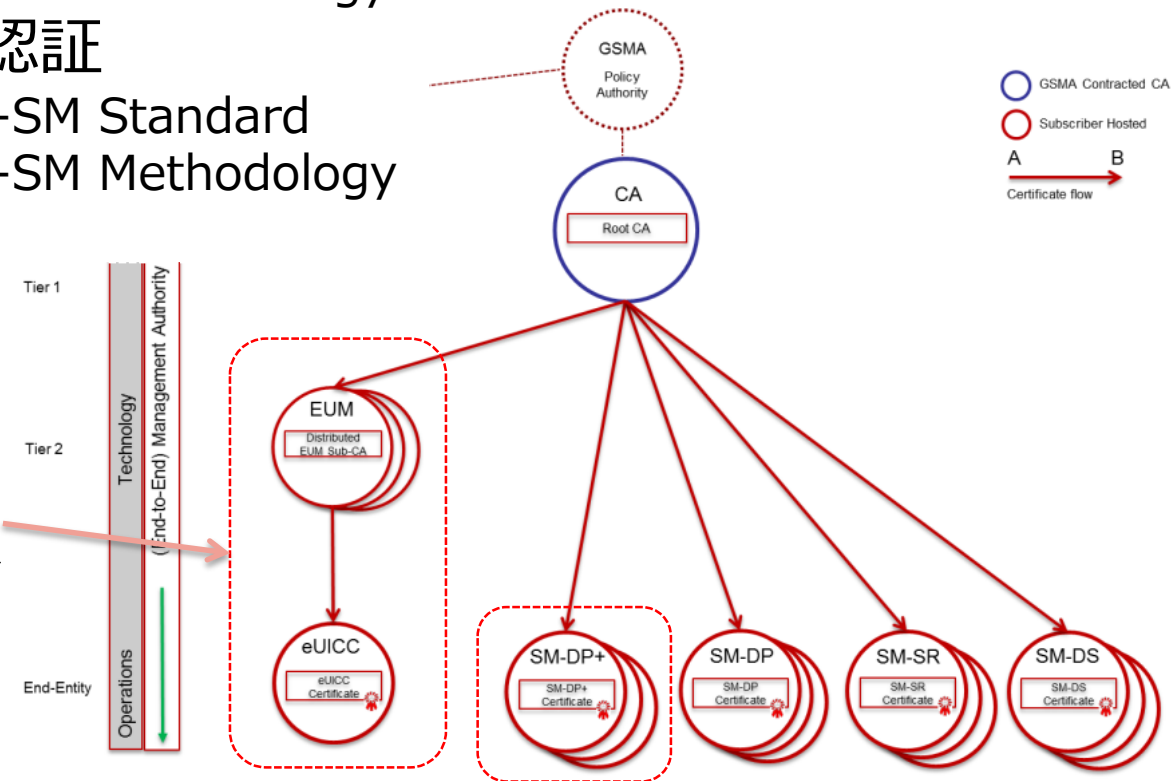


SGP.14 2.3 PKI Participants から引用

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

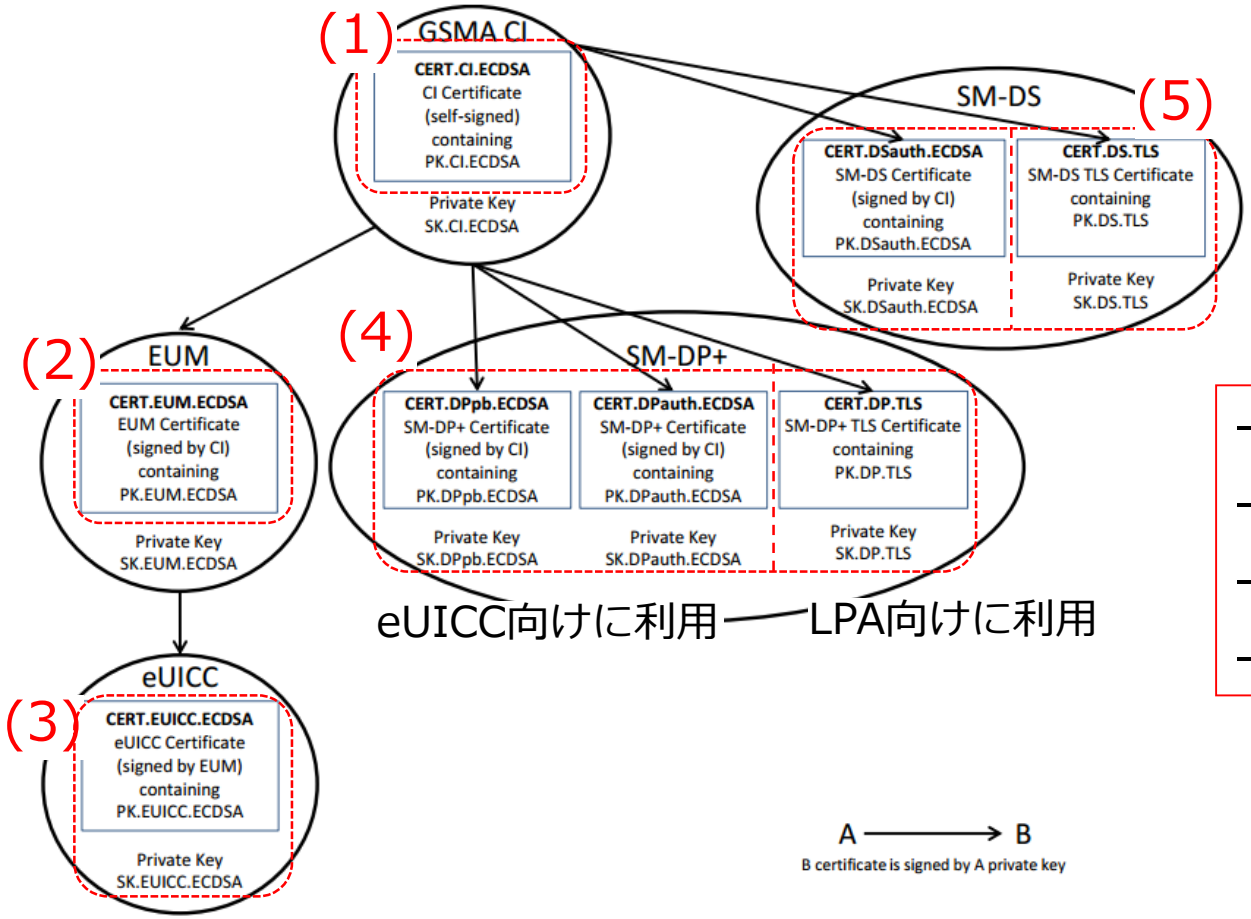
eUICCは量産するので中間認証局(EUM)で証明を受けて、個々のeUICCはEUMで署名する



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



- eUICC: (1)+(2)+(3)
- SM-DP+: (1)+(4)
- SM-DS: (1)+(5)
- LPA: (1)

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

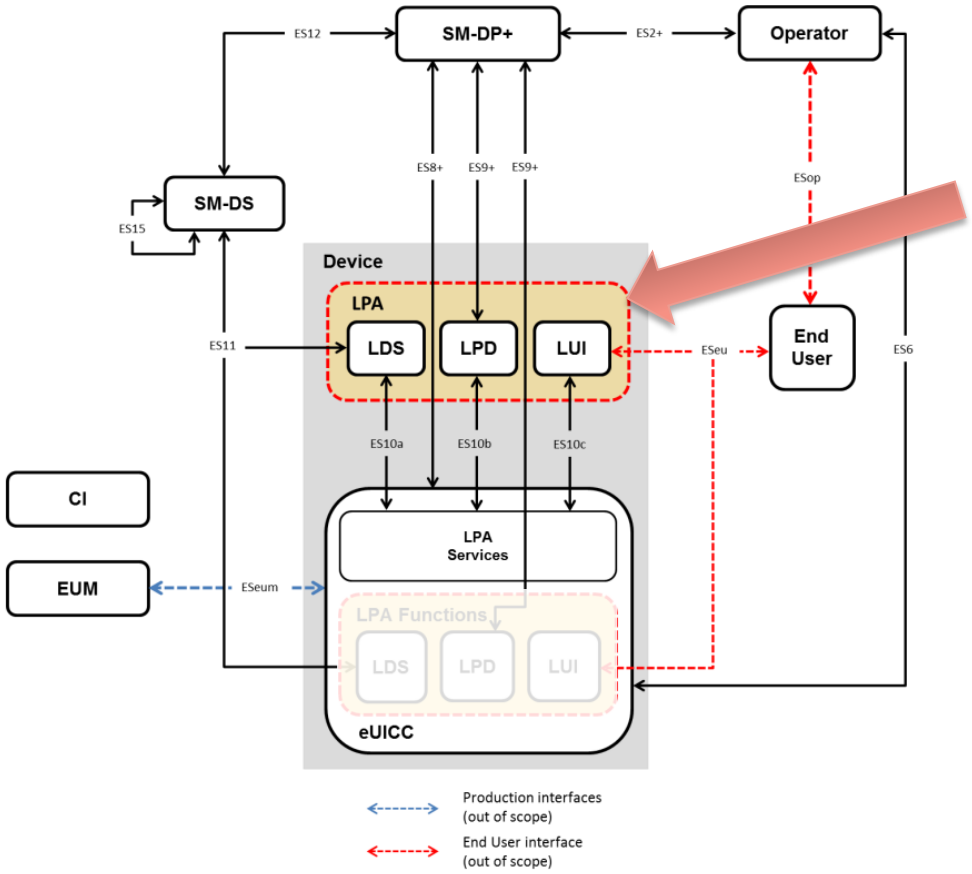


Figure 1: Remote SIM Provisioning System Architecture

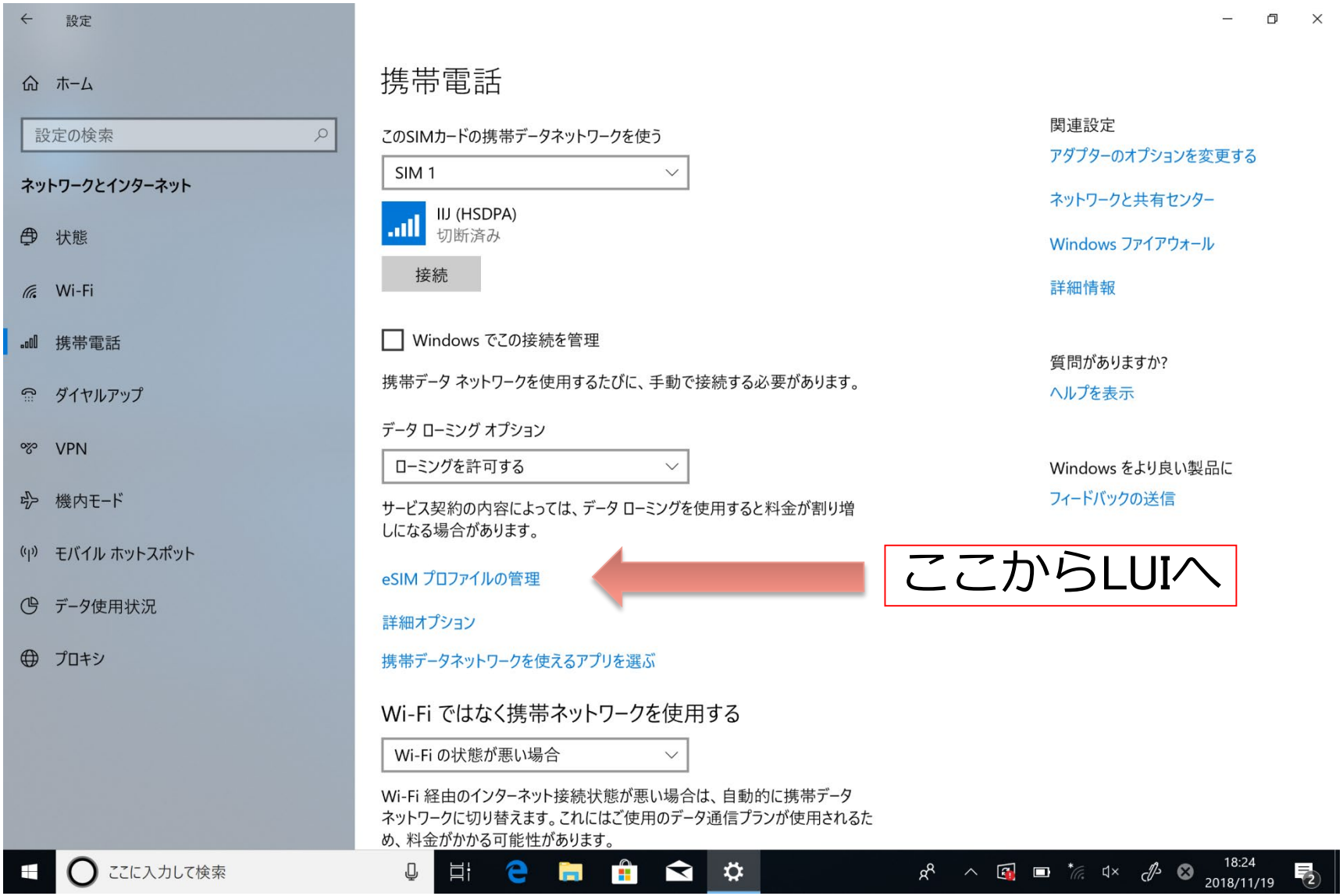
SGP.21より引用

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

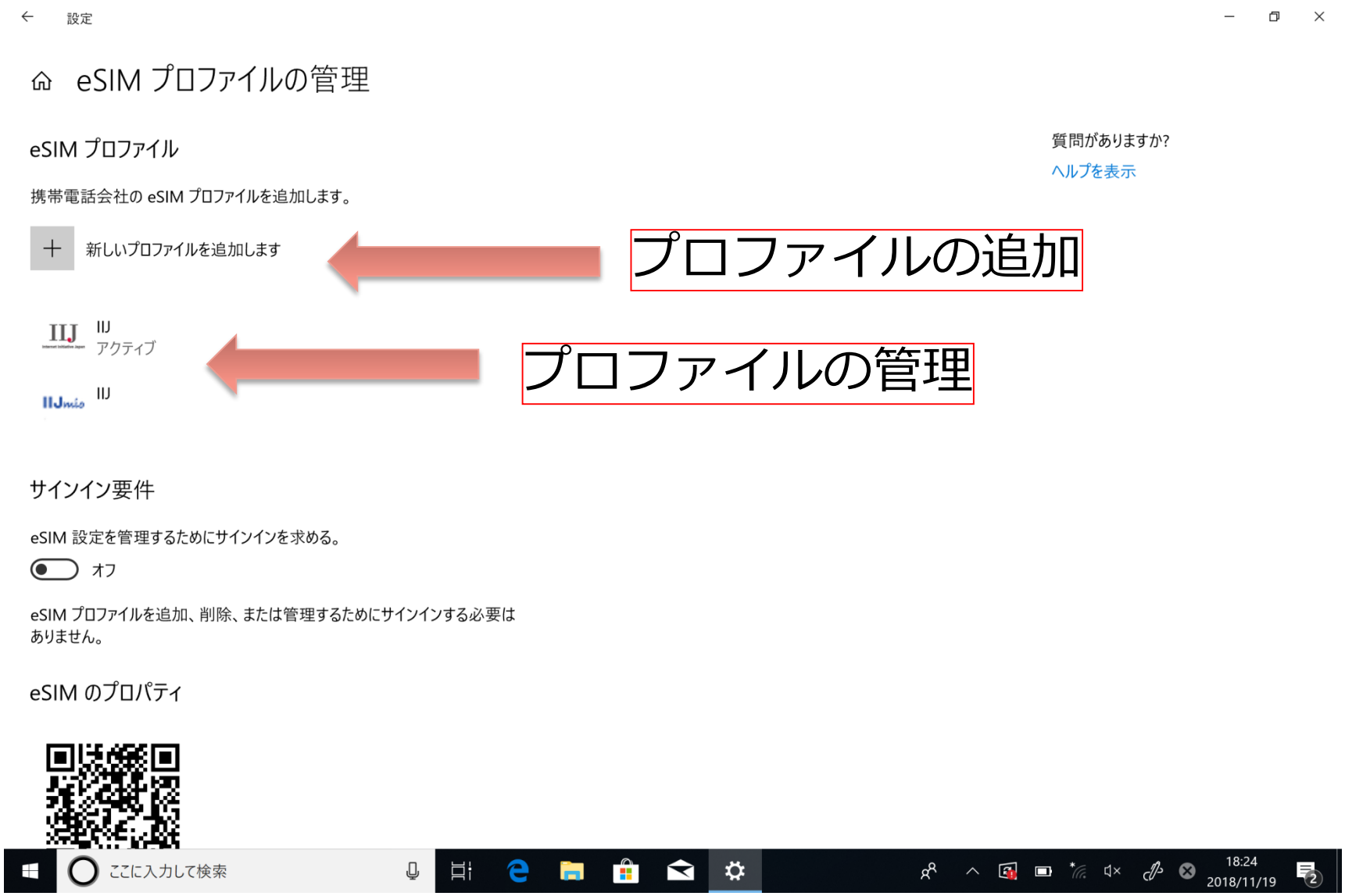
３種類の機能に分類される。

- 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に問い合わせて、自身のeSIM(EID) 宛にイベントがないかを確認する

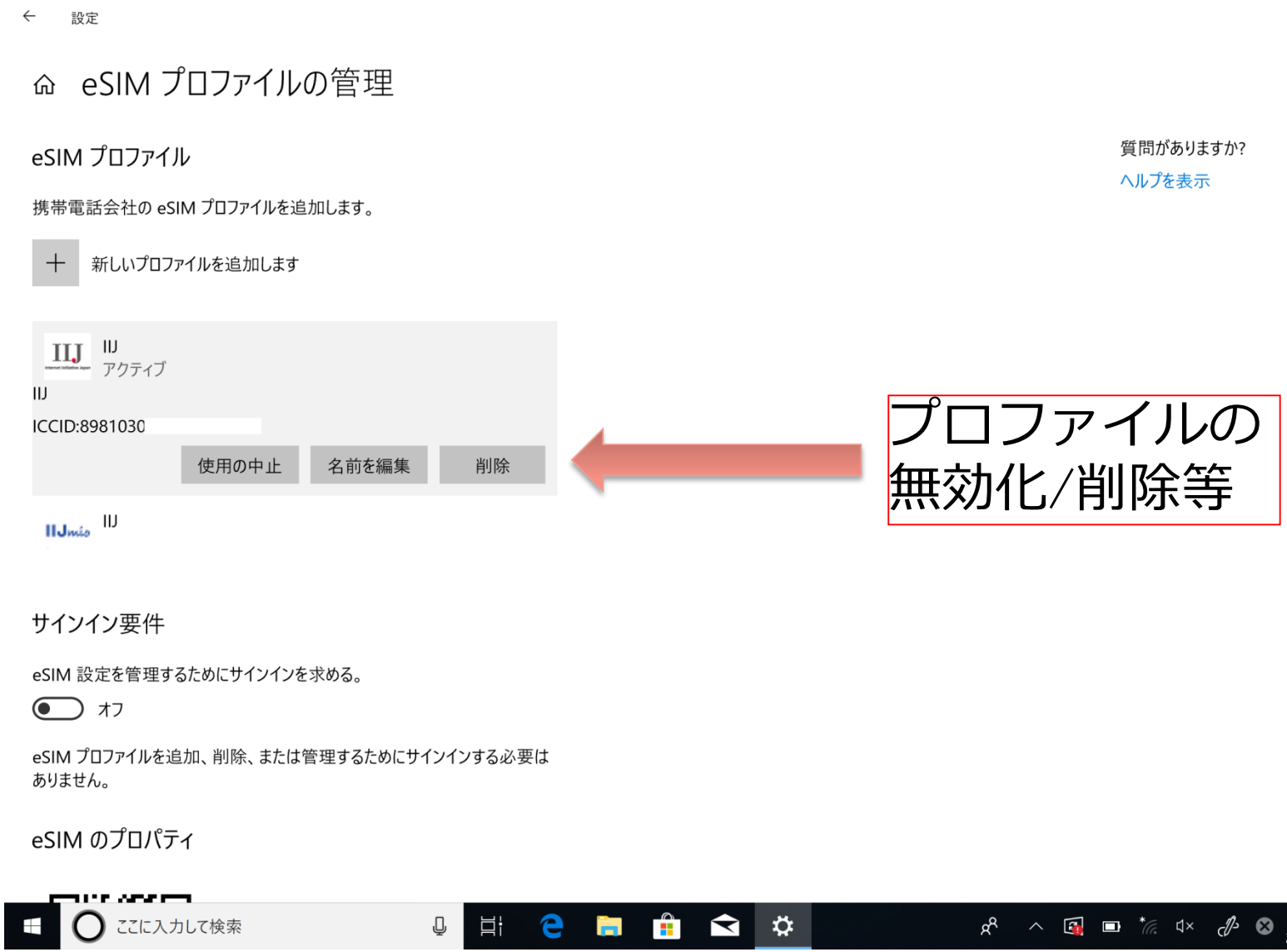
LPAとは - 2 / LUIの例



LPAとは - 3 / LUIの例

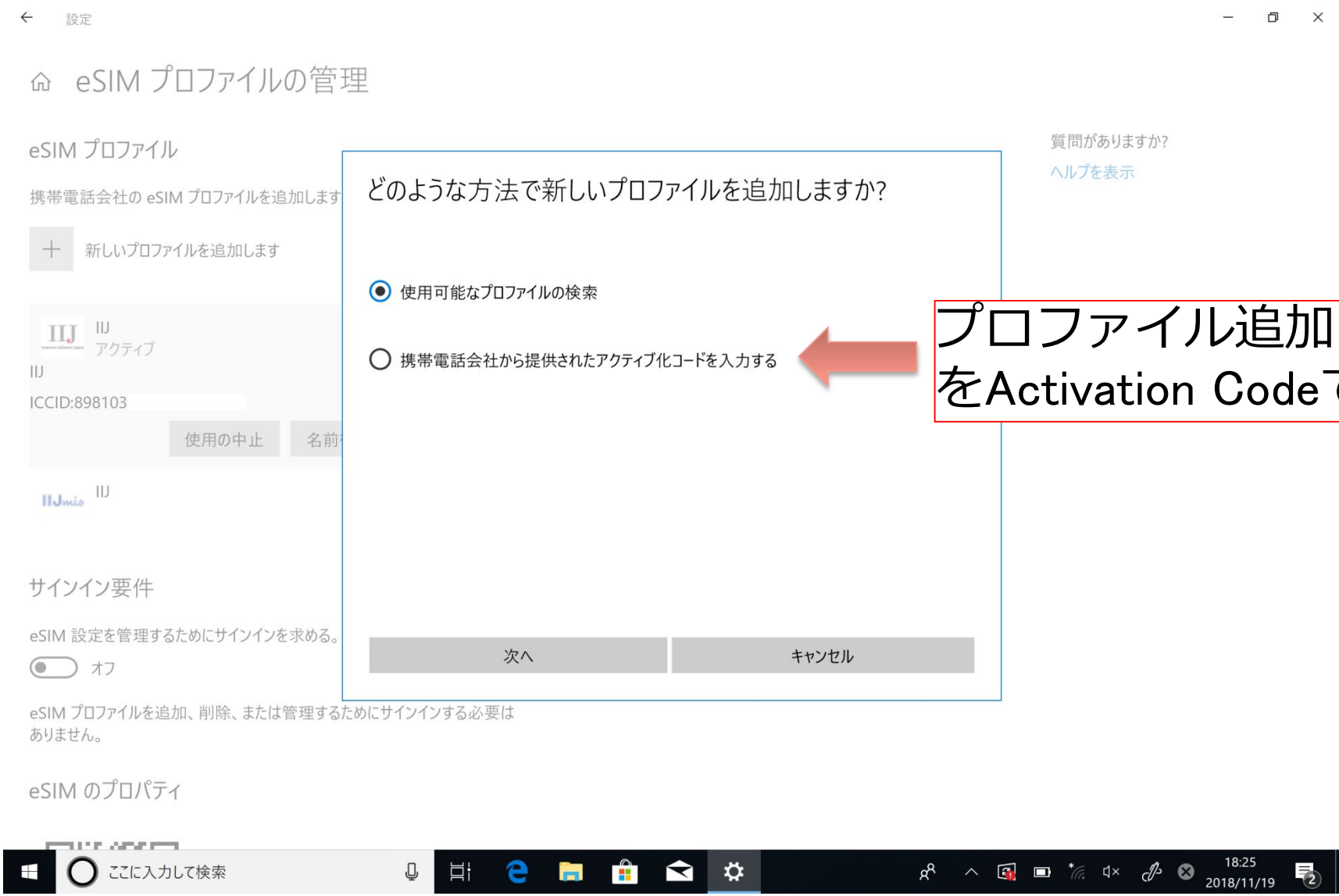


LPAとは - 4 / LUIの例



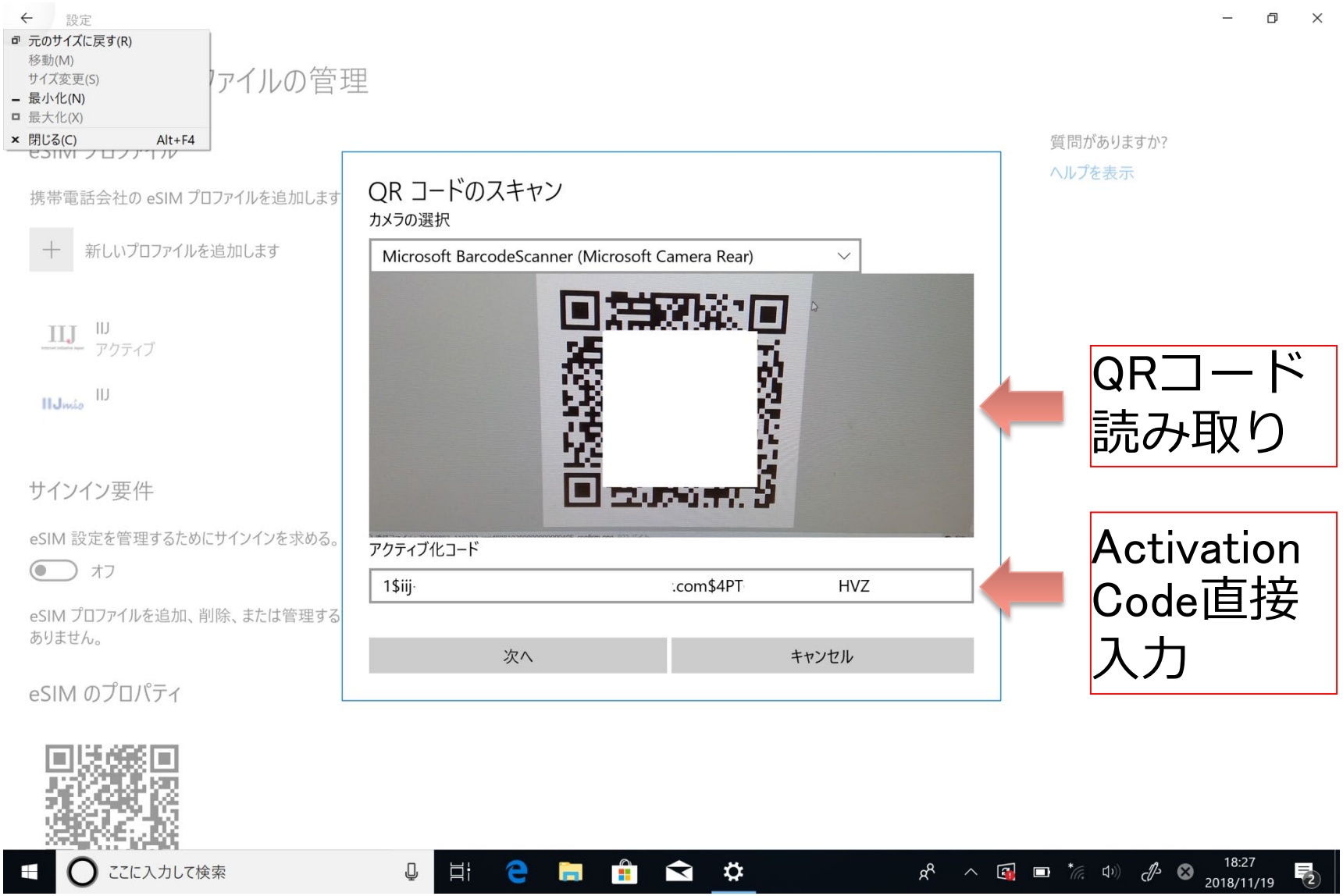
プロファイルの
無効化/削除等

LPAとは - 5 / LUIの例



プロファイル追加をActivation Codeで

LPAとは - 6 / LUIの例



QRコード読み取り

Activation Code直接入力

LPAとは - 7 / LUIの例

LUIの問題点: QRコード読み込み問題

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
     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

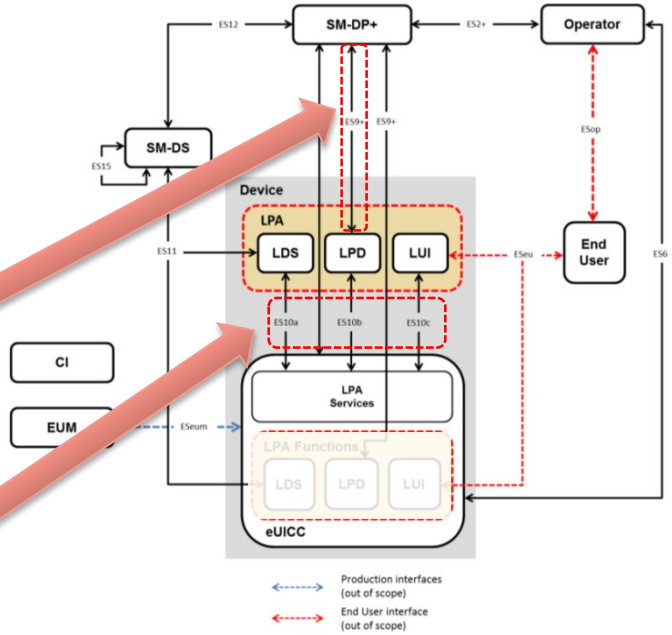


Figure 1: Remote SIM Provisioning System Architecture

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" : "8981030000000xxxxxxF",
}
```

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" : "8981030000000xxxxxxF",
}
```

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.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"
  }
  "releaseFlag": true,
  "iccid" : "8981030000000xxxxxxF",
}
```

確保したプロフィアルをダウンロード可能な状態にする

IIJ 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":"iij-xxxxxxxxx.com"
}
```

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

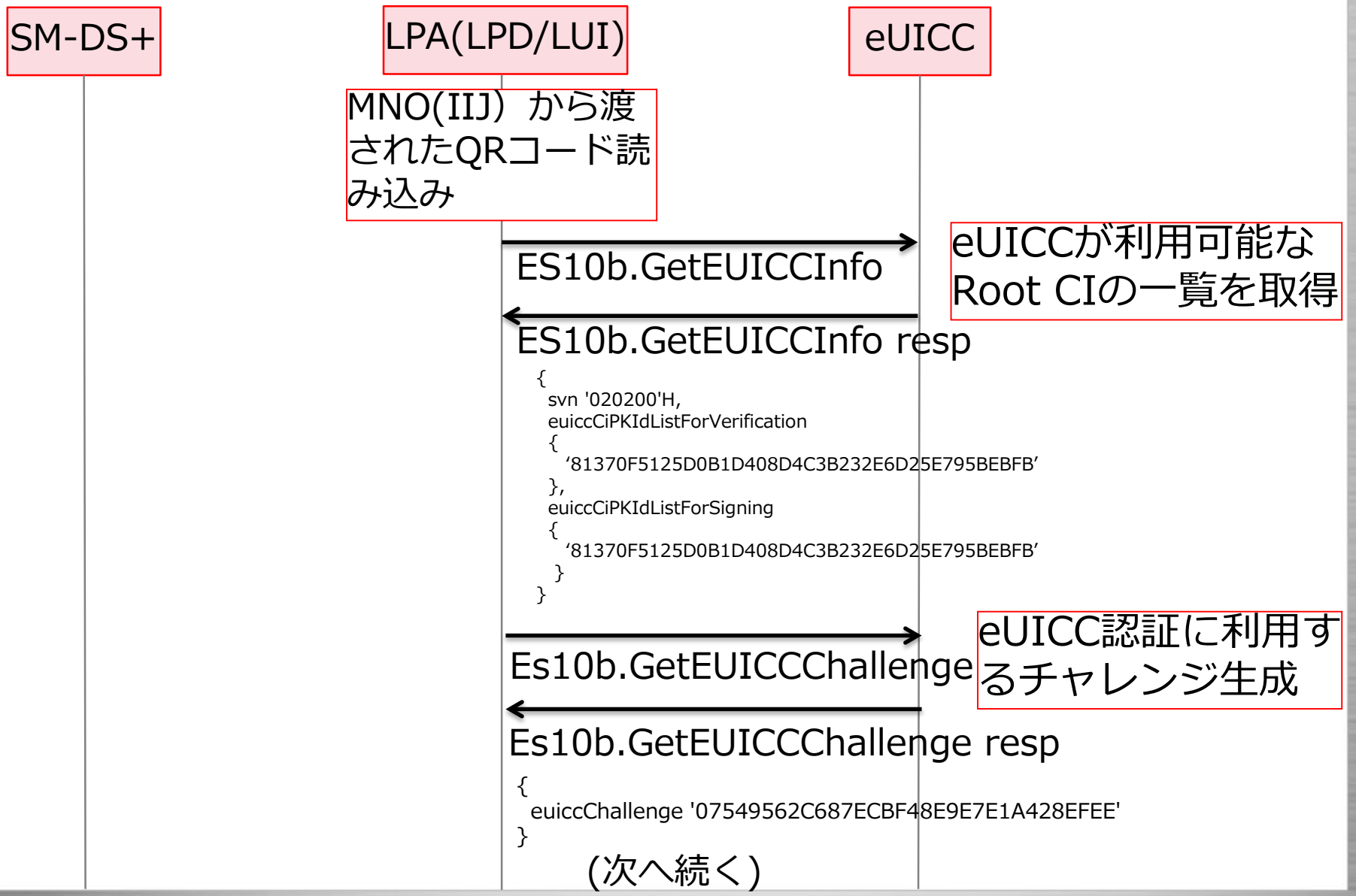
を取得。
(注) MNO側が Matching ID をしているすることも可能

QRコードを生成してユーザに渡す。
例)
LPA:1$iij-xxxxxxxxx.com$2C86-927F-XXXX-XXXX

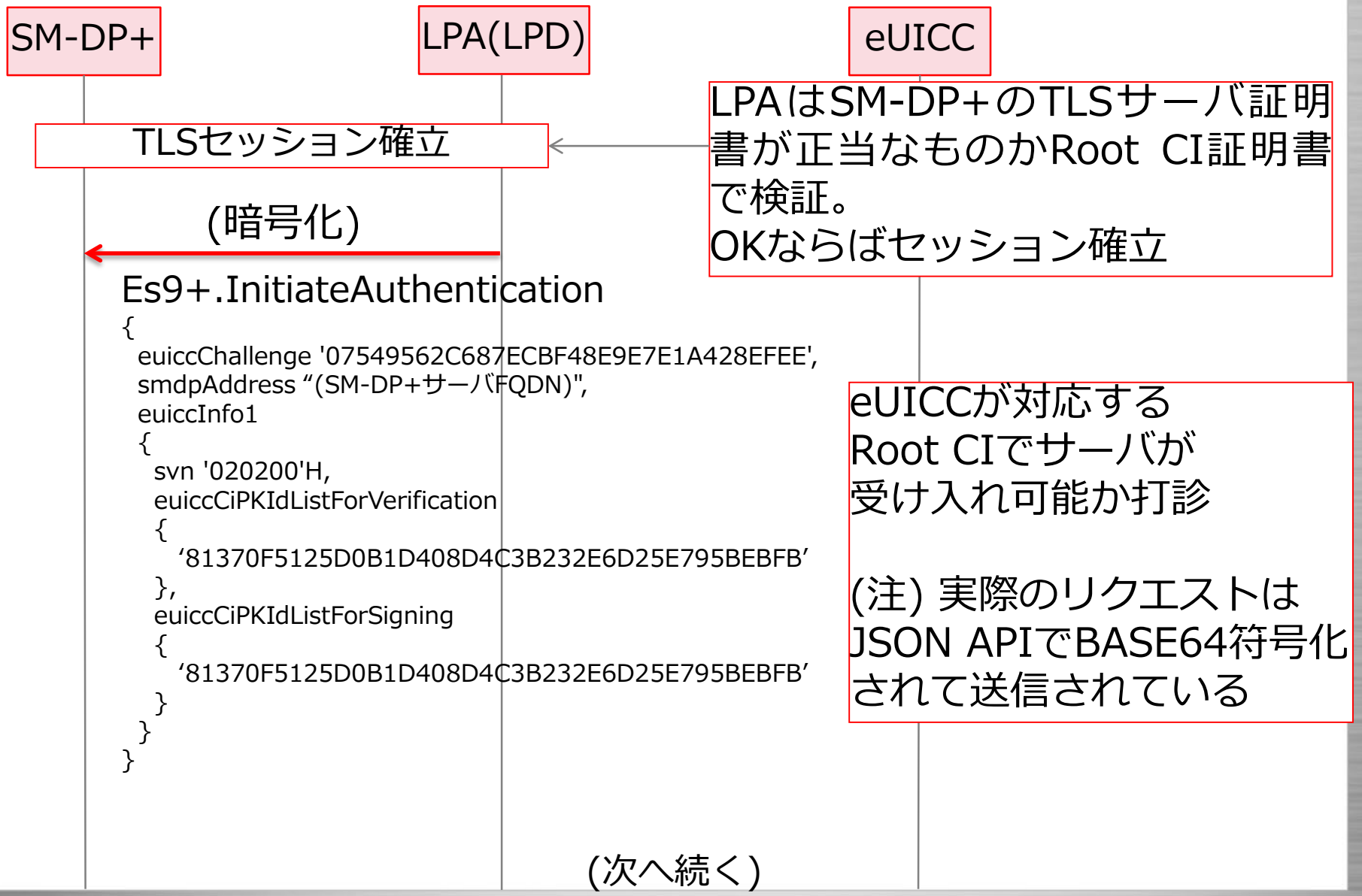
QRコード生成

(次へ続く)

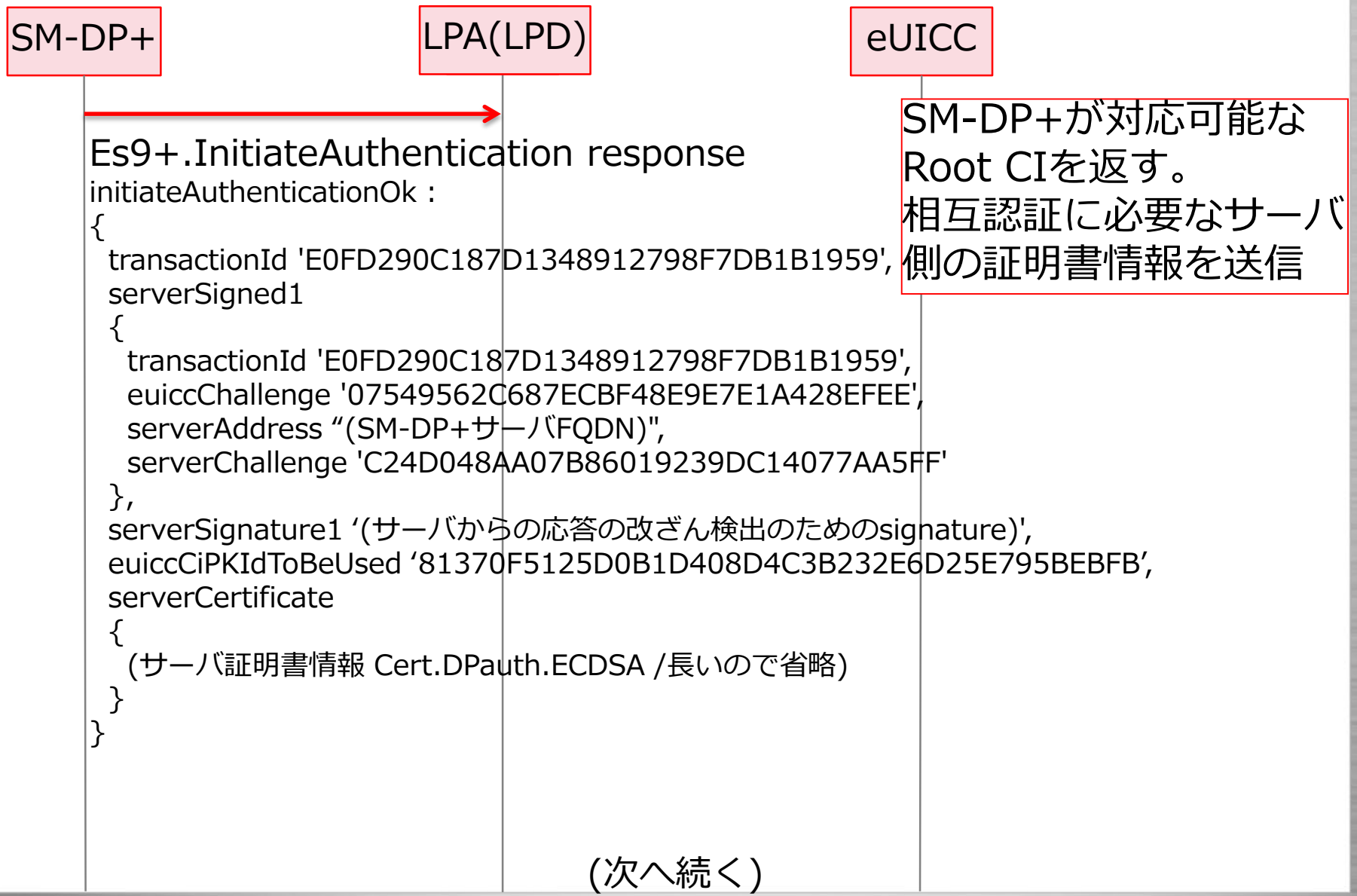
LPAとは - 11 / LPDの例



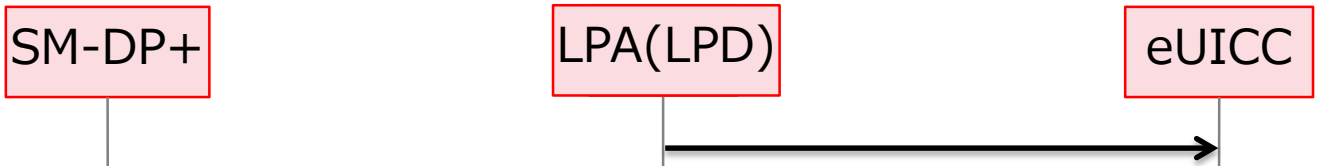
LPAとは - 12 / LPDの例



LPAとは - 13 / LPDの例



LPAとは - 14 / LPDの例

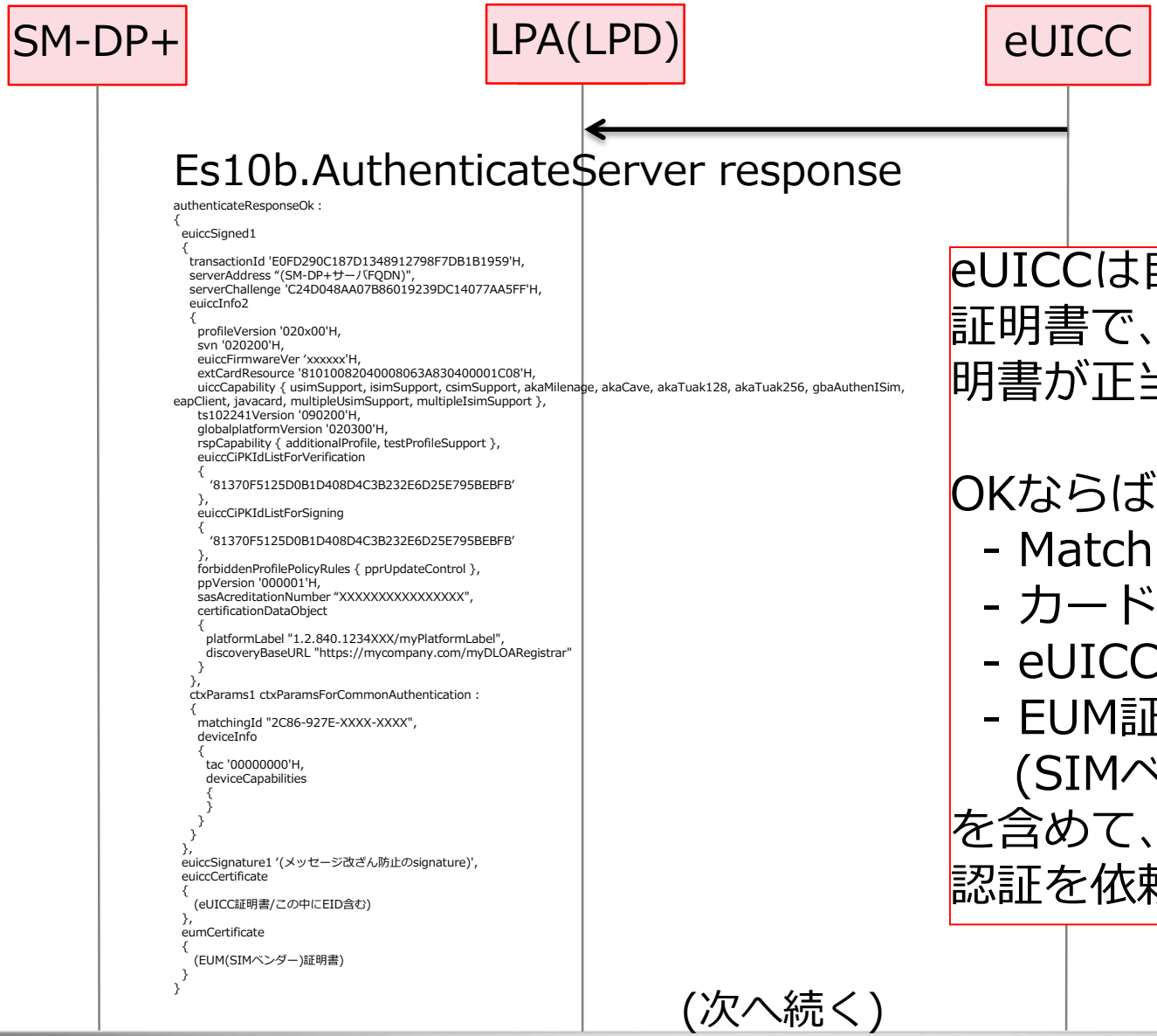


Es10b.AuthenticateServer
{
serverSigned1
{
transactionId 'E0FD290C187D1348912798F7DB1B1959',
euiccChallenge '07549562C687ECBF48E9E7E1A428EFEE',
serverAddress “(SM-DP+サーバFQDN)",
serverChallenge 'C24D048AA07B86019239DC14077AA5FF'
},
serverSignature1 ‘(サーバからの応答の改ざん検出のためのsignature)',
euiccCiPKIdToBeUsed ‘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
{
}
}
}
}

(次へ続く)

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

LPAとは - 15 / LPDの例

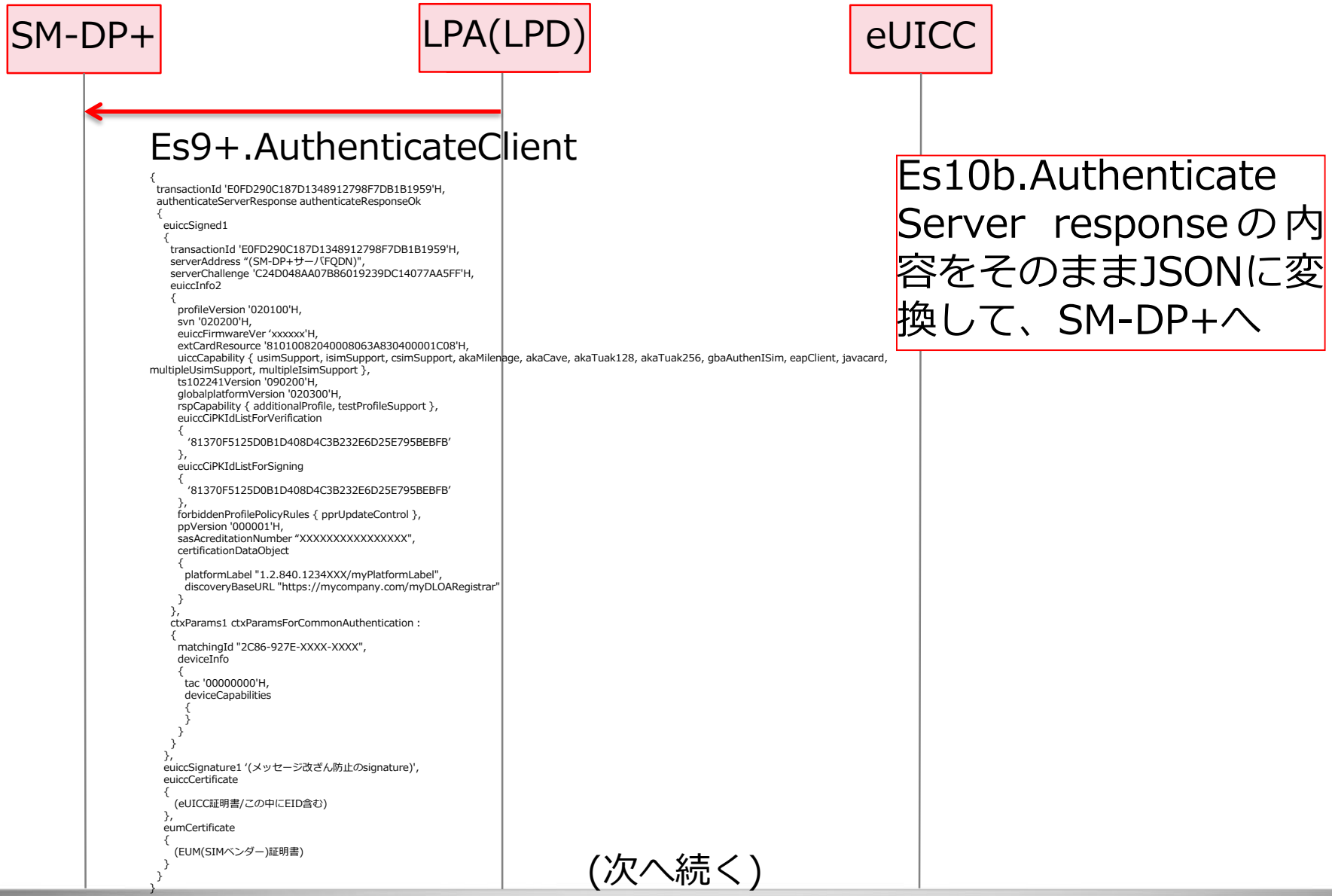


eUICCは自身の持つRoot CI証明書で、SM-DP+サーバ証明書が正当なものか検証。

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

LPAとは - 16 / LPDの例



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)
  }
}
```

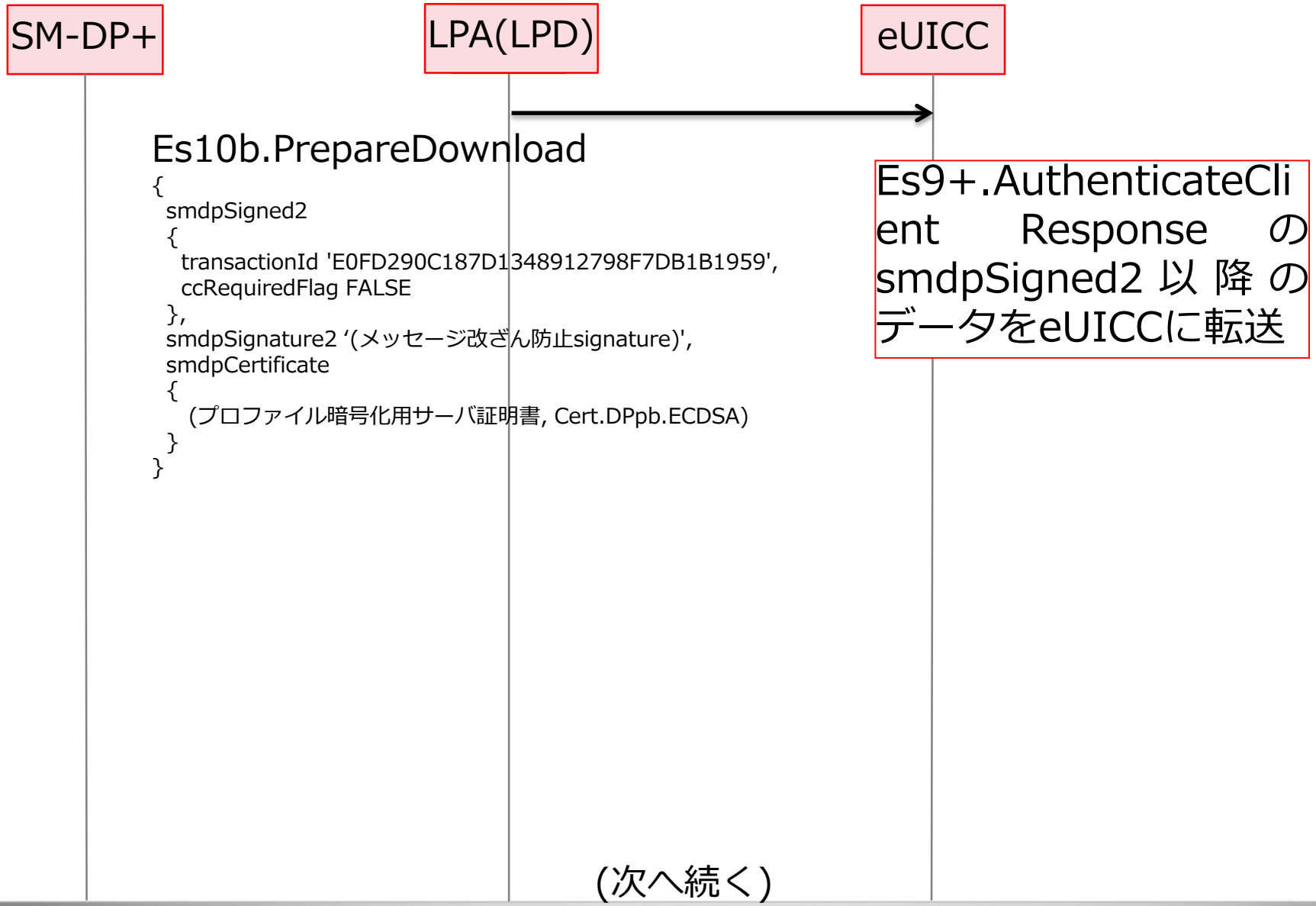
サーバ側でeUICCの正当性の確認、および、Matching IDに紐づくプロファイルが存在するか確認。

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。

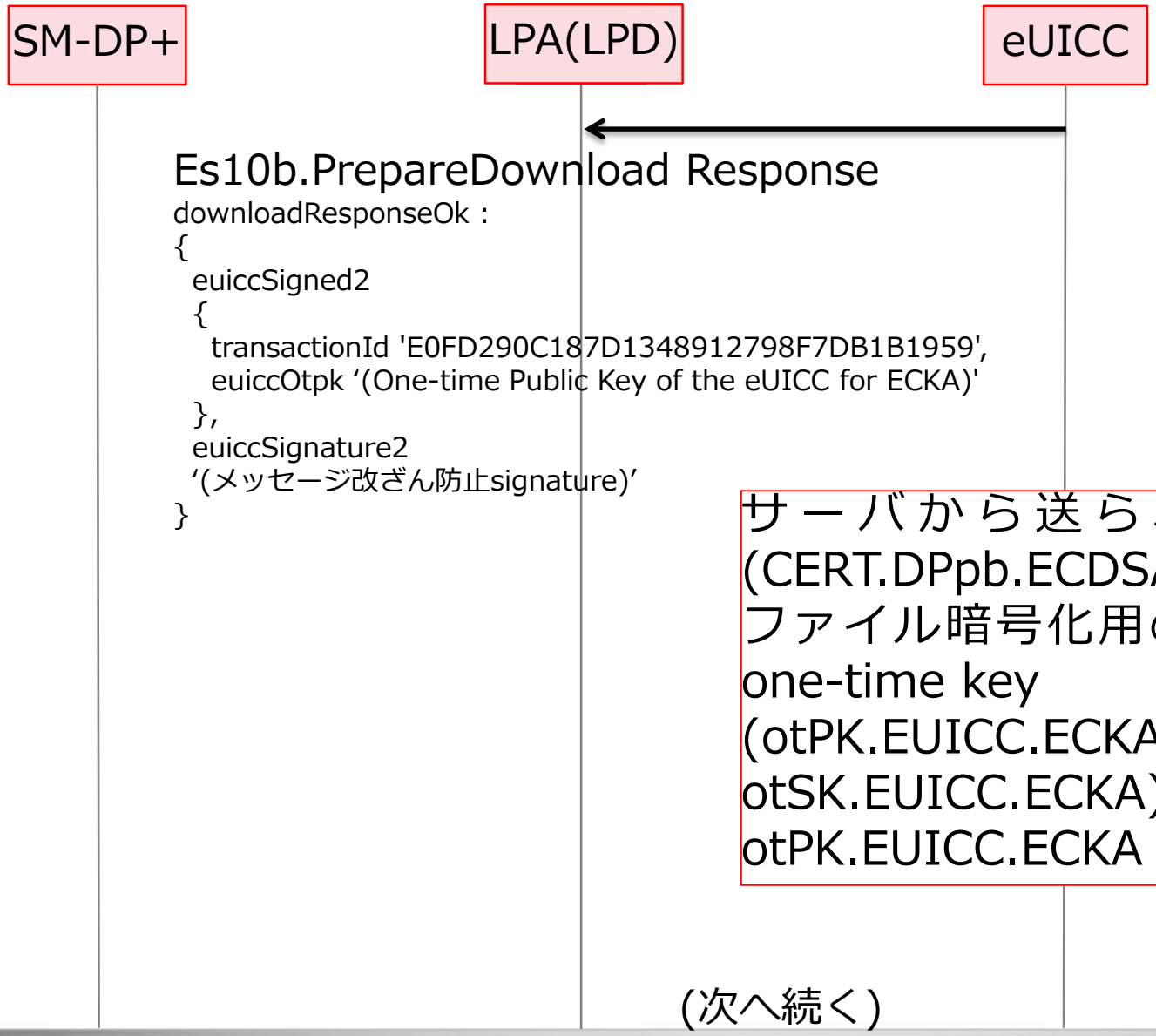
また、プロファイル暗号化のためのサーバ証明書(Cert.DPpb.ECSAD)を送信。

(次へ続く)

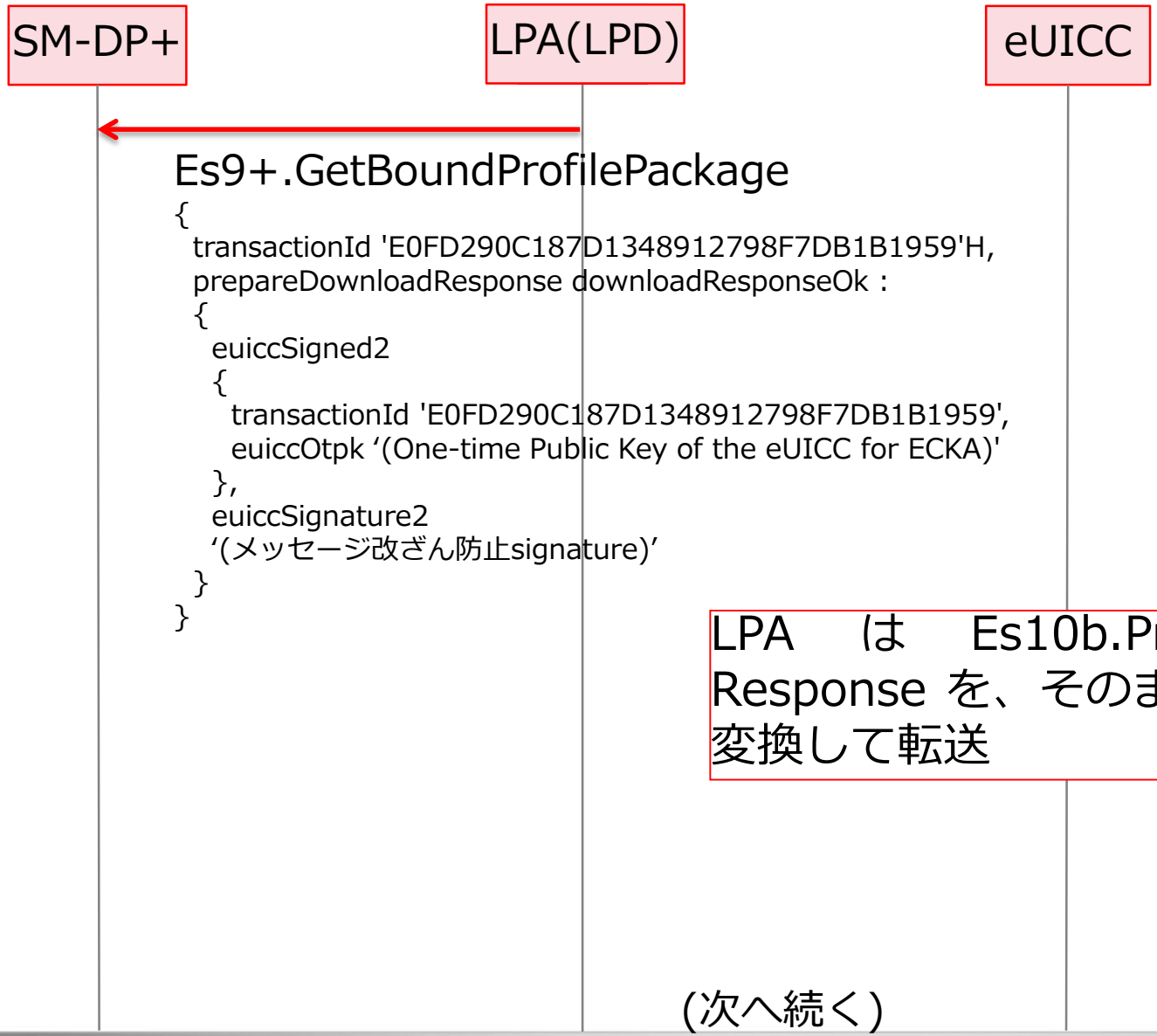
LPAとは - 18 / LPDの例



LPAとは - 19 / LPDの例



LPAとは - 20 / LPDの例



LPAとは - 21 / LPDの例

SM-DP+ | LPA(LPD) | eUICC

IIJ Profile <-> EID Downloaded

Es9+.GetBoundProfilePackage response

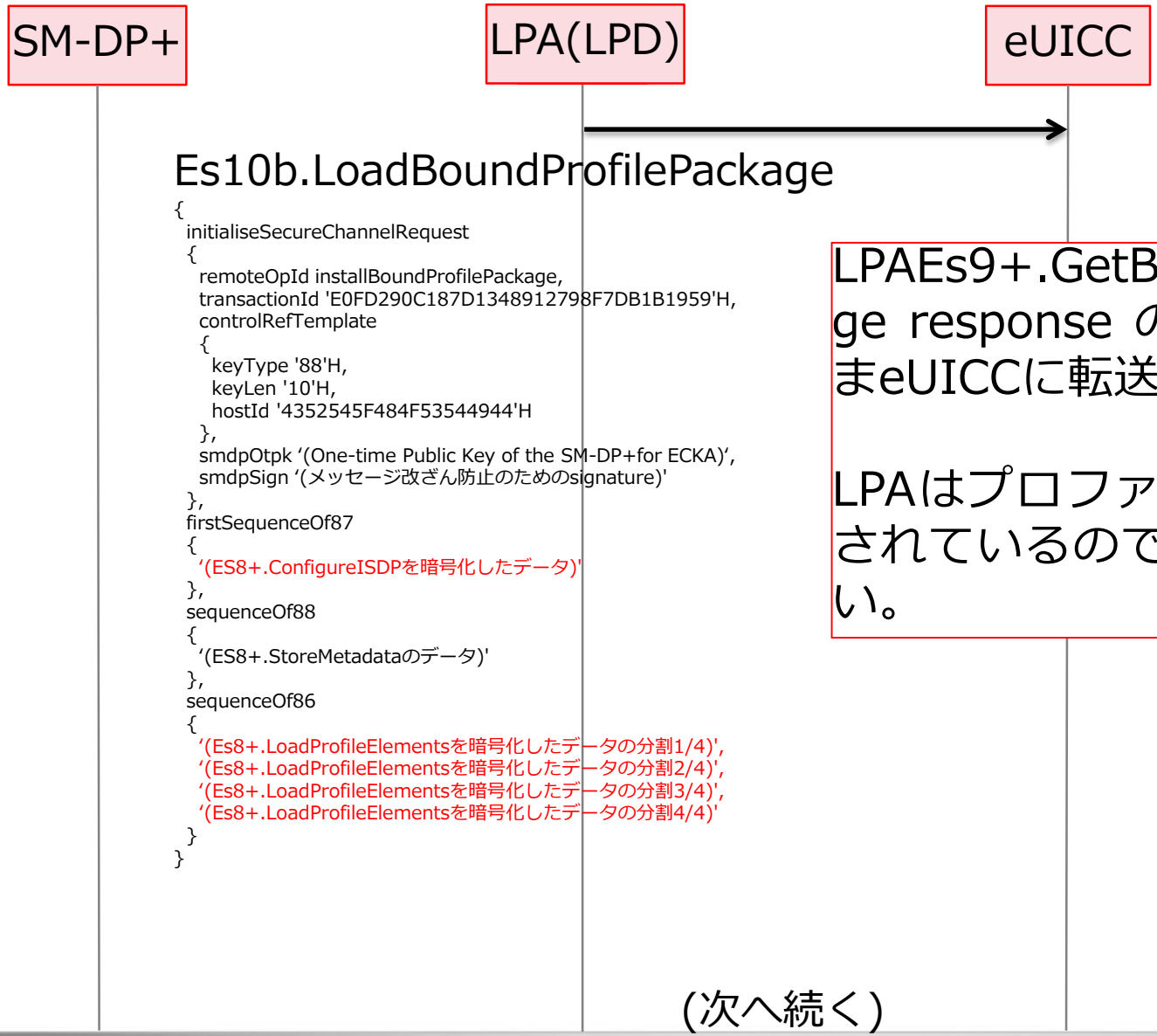
```
getBoundProfilePackageOk :
{
  transactionId 'E0FD290C187D1348912798F7DB1B1959'H,
  boundProfilePackage
  {
    initialiseSecureChannelRequest
    {
      remoteOpId installBoundProfilePackage,
      transactionId 'E0FD290C187D1348912798F7DB1B1959'H,
      controlRefTemplate
      {
        keyType '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)

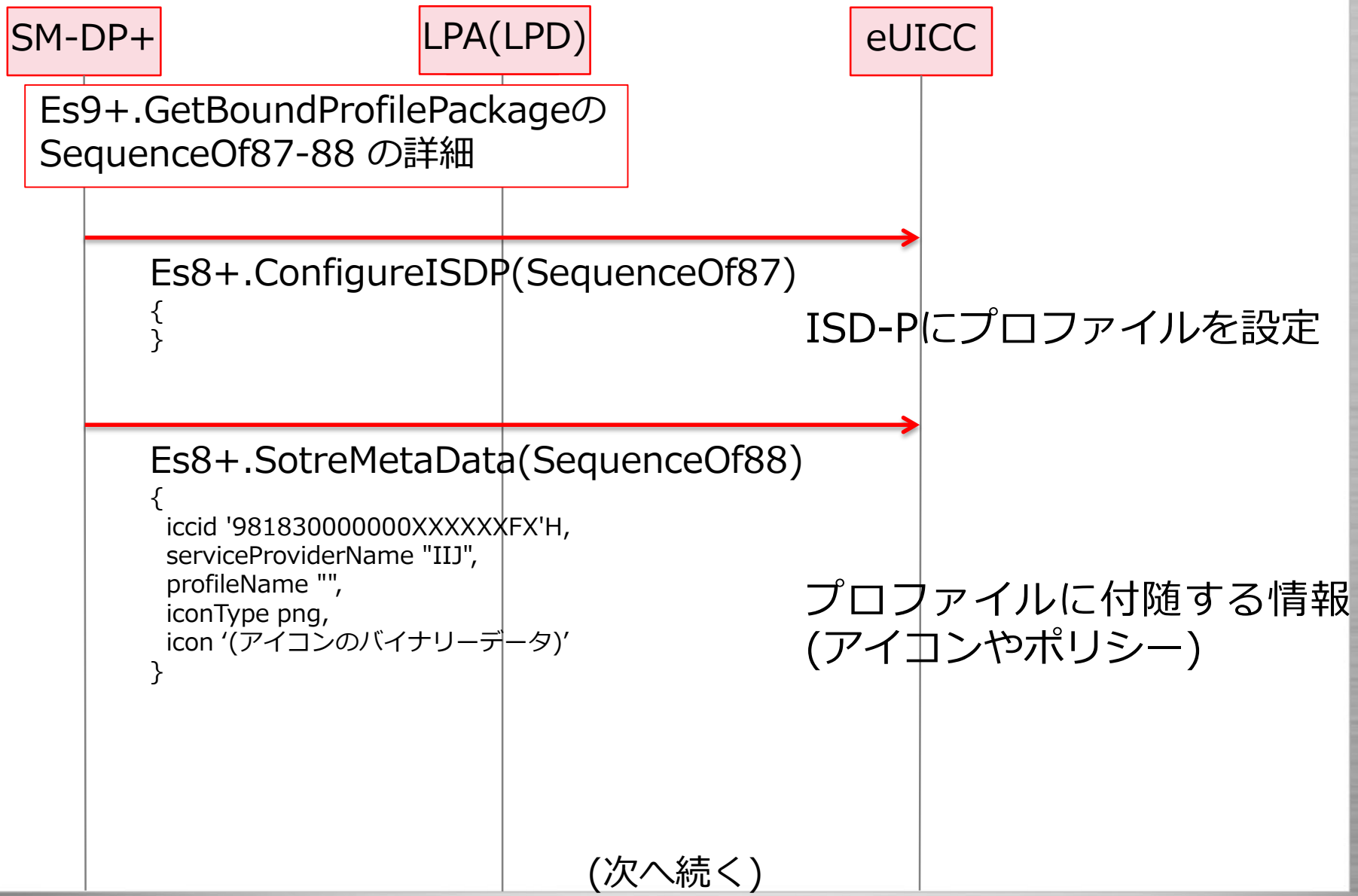
また、暗号化したプロファイルデータ等をeUICC宛に送信

(次へ続く)

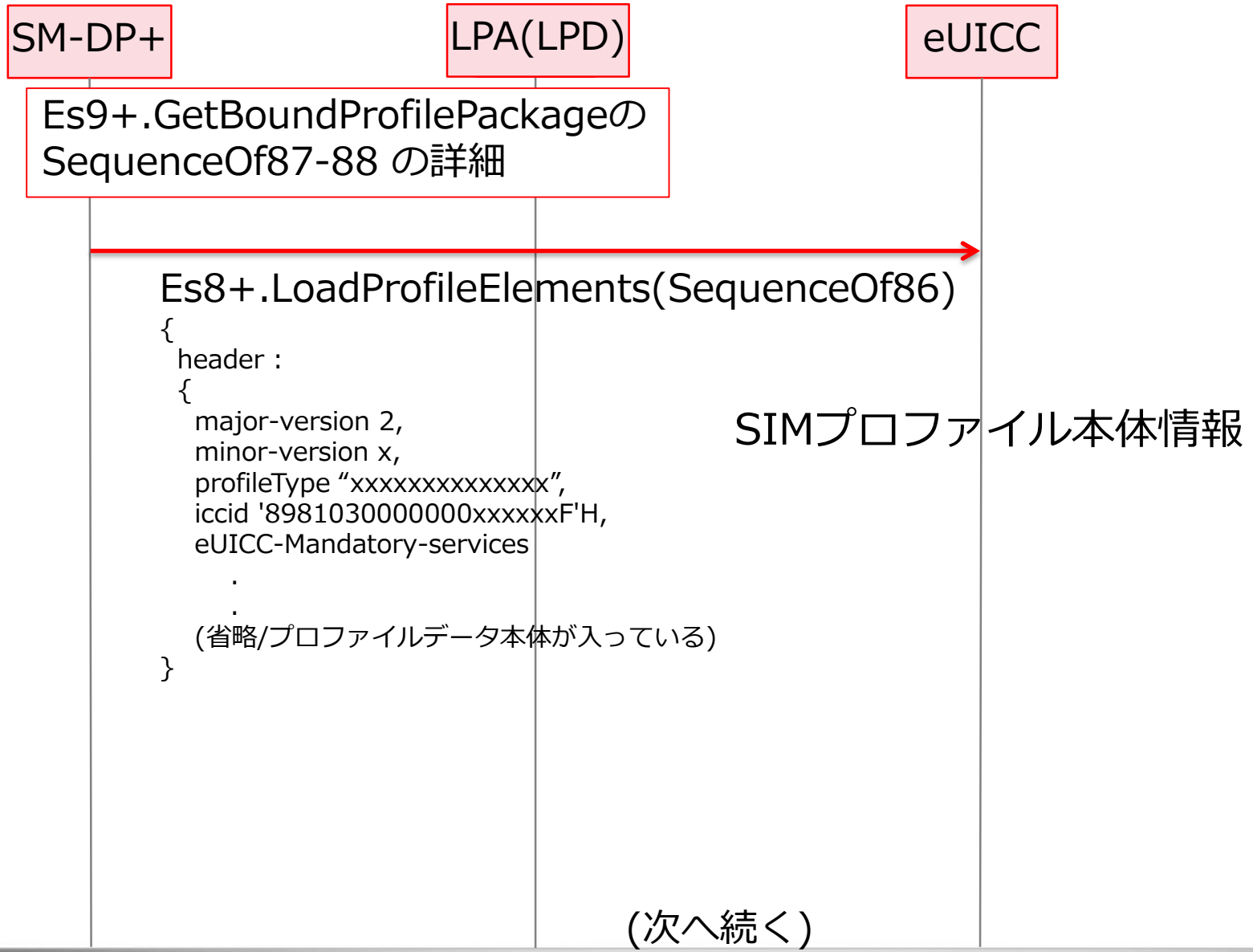
LPAとは - 22 / LPDの例



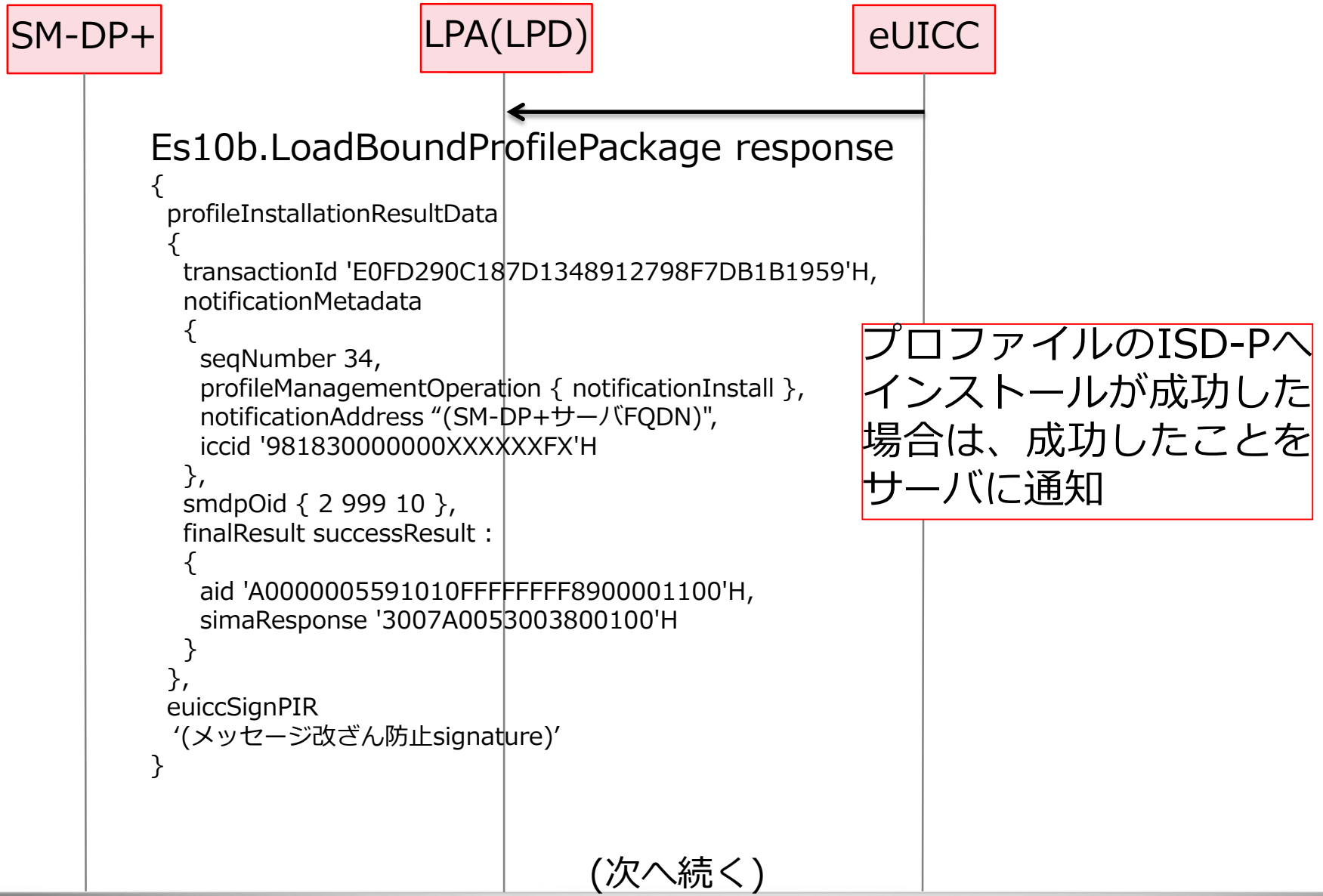
LPAとは - 23 / LPDの例



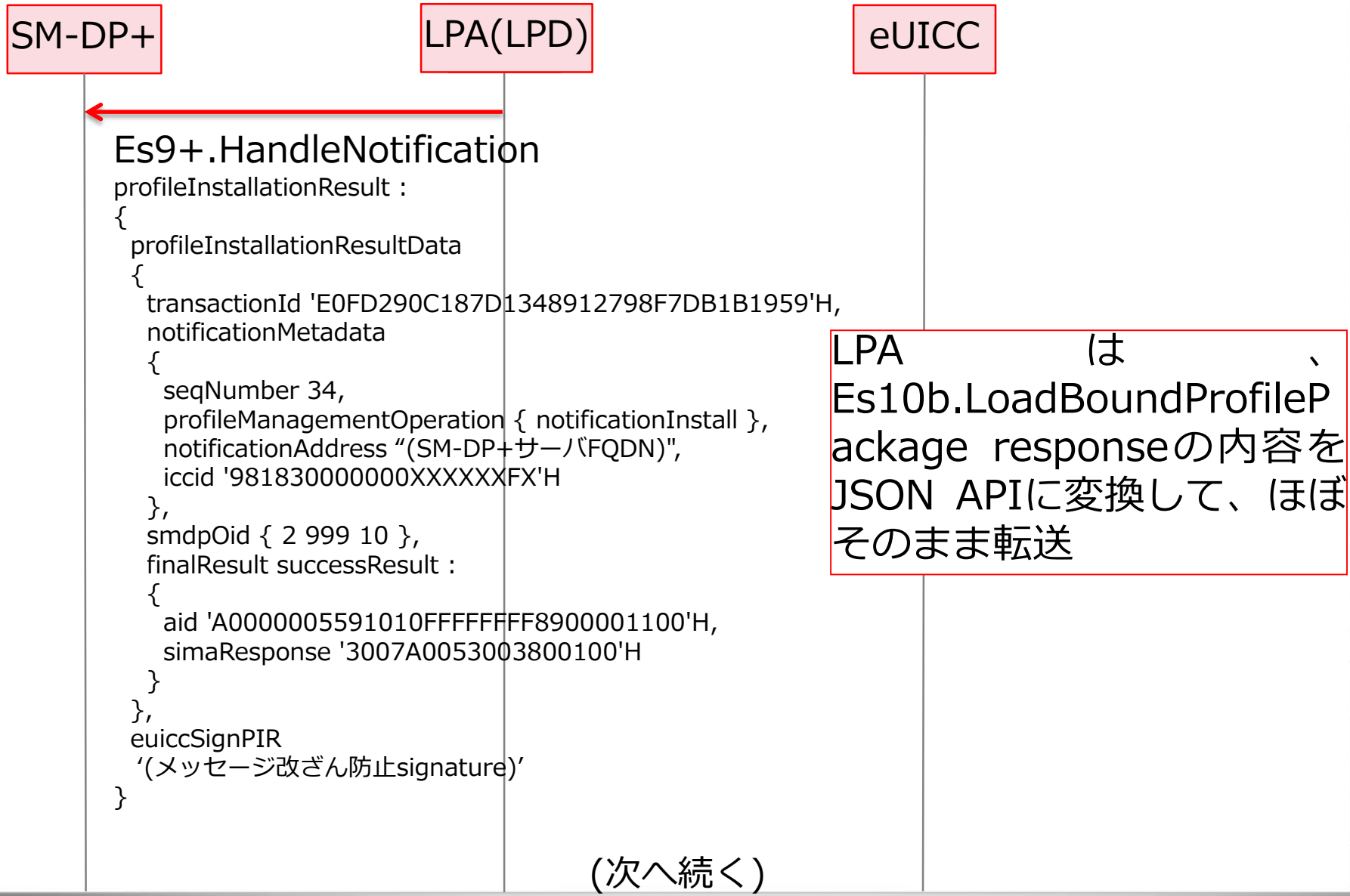
LPAとは - 24 / LPDの例



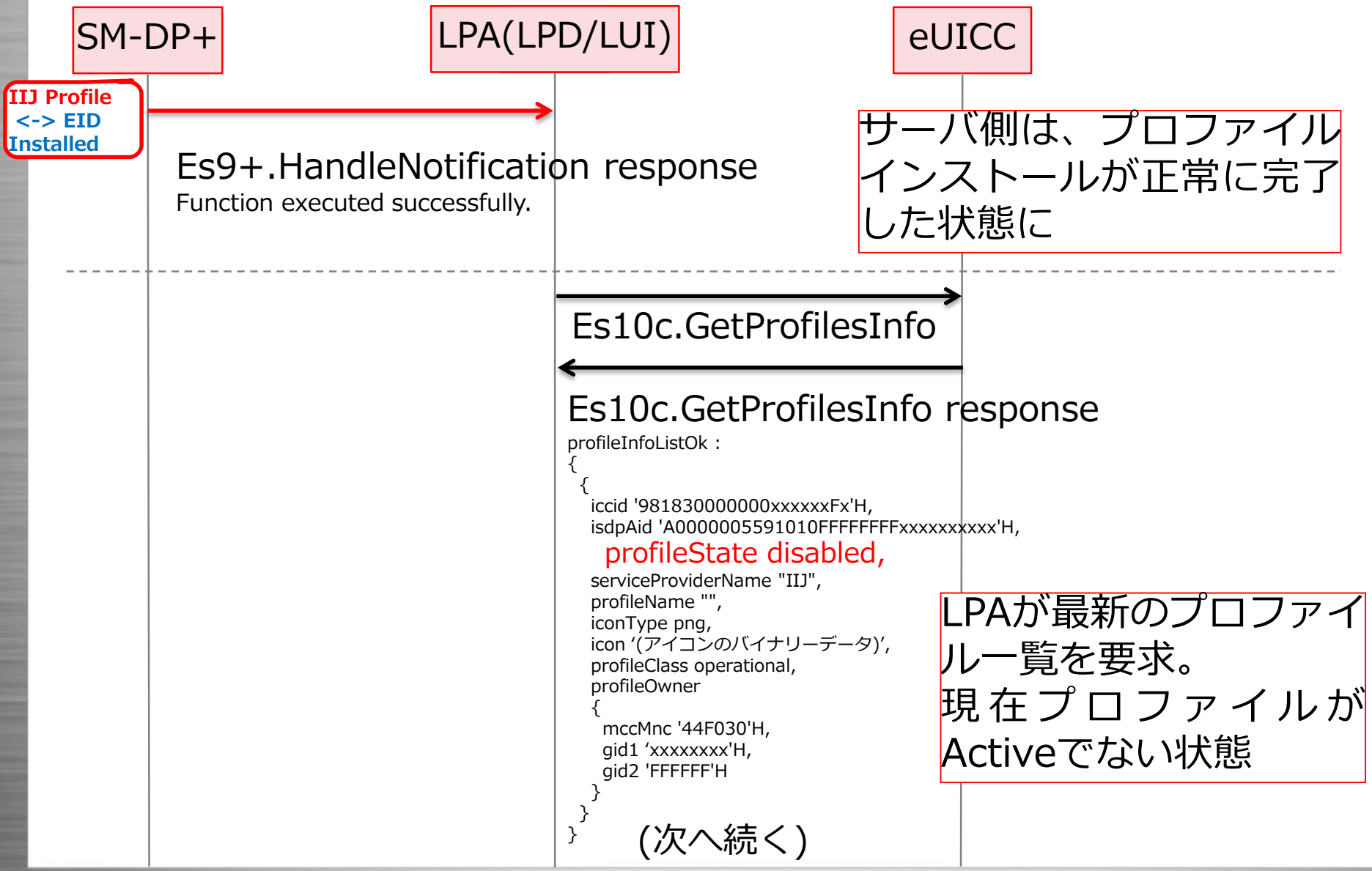
LPAとは - 25 / LPDの例



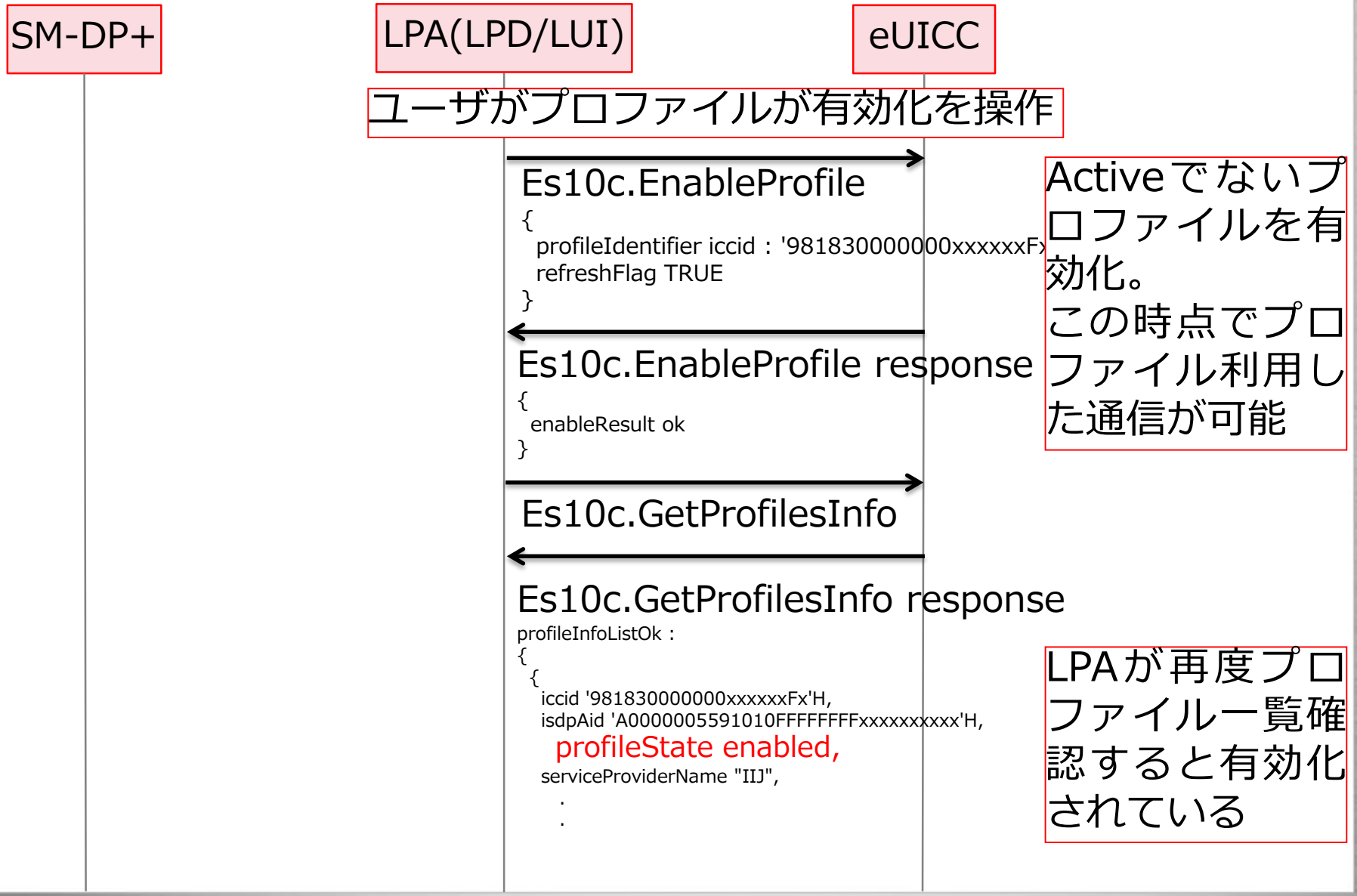
LPAとは - 26 / LPDの例



LPAとは - 27 / LPDの例



LPAとは - 28 / LPDの例



LPAとは - 29 / LPDについて

省略

PoCで実施しなかったので
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

IIJ Internet Initiative Japan

Lead Initiative

日本のインターネットは1992年、IIJとともにはじまりました。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