Commercializing eSIM for Network Operators

Bassem Ali Abdou
Netwotk Services Design
Mobily
Riyadh, Kindom of Saudi Arabia
b.abdou@mobily.com.sa

Abstract— **This paper illustrates how MNOs (mobile network operators) and MVNOs (mobile virtual network operators) can accommodate consumer devices that are equipped with embedded subscriber identity module (eSIM). It overviews the different deployment options for MNOs and MVNOs, implications on provisioning &activation systems, and associated process requirements. A fast track option would be cloud-based and relying on pre-printed eSIM vouchers; a standard deployment mechanism would be relying on on-demand generated eSIM vouchers; a sophisticated and complex deployment would involve a device entitlement gateway platform; finally, and though no known reference is using it, a discovery service based deployment is also an option. The paper includes eSIM reflections on SIM-related customer operations and highlights the need to introduce new eSIM re-use mechanism, the part that is still unavailable in GSMA (GSM association) specifications.**

Keywords—eSIM, eUICC, RSP, SM-DP+

I. Introduction

Among wider set of stored information, any SIM (subscriber identity module) typically hosts two types of information: authentication information and identity information such as ICCID (integrated circuit card identifier) and IMSI (international mobile subscriber identity). From 1991 to 2012, SIM evolved from the 1FF variant, to the 2FF (mini SIM), to the 3FF (micro SIM), and to the 4FF variant (nano SIM) [1]. Though those transitions led to removable physical SIMs of smaller sizes, major benefit was at device manufacturers side as they could optimize the hardware. Operator benefits and processes remained almost untouched.

The latest evolution from physical SIM to eSIM (embedded SIM) allowed the separation between the physical chipset on the device and the operator's profile. Devices can be produced with built-in chipsets that have no operator profile or have an initial profile that could be changed in a later stage. Prior to the actual usage of the SIM, and depending on the location and device owner, new MNO (mobile network operator) or MVNO (mobile virtual network operator) profile could be downloaded over internet. In order to achieve this, provisioning and downloading processes should be standardized in a way that will ensure integrity, security and inter-operability are in place.

It should be clear that eSIM does not only imply new technology; it also implies new business process [2]. Devices can be under one of the following two categories:

- Category-I, where the user has full control on which operator profile is to be downloaded on the device; mobile phones, laptops and some IOT (internet-of-things) devices such as smart watches and other user-owened wearables fall under this category.
- Category-II, which includes IOT devices where manufacturers or IOT service providers have control over which operator profile is to be pushed to the device. Many M2M (machine-to-machine) solutions such as smart meters and cars fall under this category.

The pull mechanism used with devices under category-I assumes full control at the device (and accordingly user) and provides local capability to pull the operator profile he/she selects. Category-II devices on the other side shall provide manufacturers and IOT operators the capability to remotely push the right profile to the device in a seamless way. Such difference between the two categories led to the emergence of two RSP (remote SIM provisioning) standard tracks produced by GSM Association: RSP Technical Specifications for Consumer Devices [3] (covering category-I) and RSP Specifications for M2M [4] (covering category-II). As of the date this paper is written, RSP Technical Specifications Release 2.2 is the latest GSMA document for consumer eSIM (issued in September 2017), while Remote Provisioning Architecture for eUICC (embedded universal integrated circuit card) Technical Specification version 3.1 is the latest GSMA document for M2M eSIM (issued in May 2016).

This paper will focus on commercializing eSIM for MNOs and MVNOs in the light of GSMA's RSP Technical Specifications Release 2.2 for consumer eSIM devices, a market that that is expected to approach 1.5 Billion units globally by the year 2022 [5]. In specific, the different approaches to deploy SM-DP+ (subscription manager data preparation platform for consumer devices) and the options for provisioning and activating eSIMs will be illustrated, together with the impact on the business process. While eSIM should simplify activation process in specific, the fact that profiles are downloadable over the internet raises some security concern that did not exist in physical SIMs and imposes some complications when users change their handsets. The associated limitation and a recommendation for GSMA on how to enhance the standard for profile movement from a device to another will be also illustrated.

While basic ecosystem information will be included (where GSMA's RSP Technical Specifications Release 2.2 for consumer eSIM devices is the main reference), the intention is not to provide detailed and complete descriptions for components, interface protocoles, commands and parameters, which are already available in GSMA specification releases. Also the eSIM network security is beyond the scope of this paper.

II. Remote SIM Provisioning – Consumer Version

A. Architecture

Fig. 1 illustrates GSMA Architecture for the eSIM ecosystem

The architecture introduces three elements that are new to the mobile telecom world and created specifically for the eSIM:

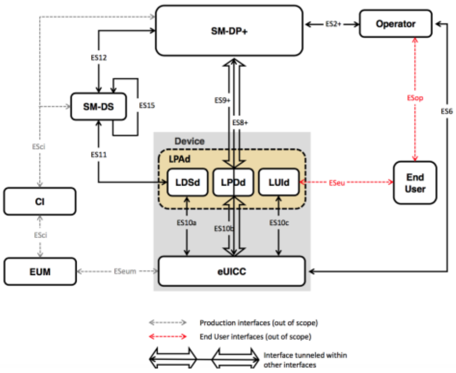

Fig. 1 Remote SIM Provisioning System [3]

- SM-DP+ is the consumer version of the subscription manager; it is responsible for hosting eSIM profiles and availing them to eSIM enabled devices. It essentially has direct interaction with the end user device and with the network operator.

- LPAd stands for local profile assistance –device version- which is a new function block in the device; it interacts with eUICC, end user and SM-DP+; it is used for downloading operator profile from SM-DP+, storing it on the eUICC, and deleting it when needed. While LPA typically comes as a default capability in the device, device operating system may have an API using which operators and 3rd parties can develop their own smartphone applications [6].

- SM-DS stands for subscription manager – discovery service, a platform that SM-DP+ notifies in advance about profile availability for certain devices; devices later on check the SM-DS for profile availability and associated SM-DP+ information. SM-DS might be run by neutral entity and is currently available at GSMA only. It's not mandatory for commercial launch of eSIM as its purpose and functionality are completely optional; till the time this paper is released, no known operator went for this kind of deployment.

B. Interfaces

The architecture includes new interfaces that have been introduced by GSMA specially for remote SIM provisioning:

- ES2+ is the interface between Operator's service fulfillment and SM-DP+ as shown in Fig. 2. It is used by the operator in order to provision eSIM profiles and make them ready for download and will be focused on in this paper. It can be also used for reporting purpose in the direction from SM-DP+ to MNO.

- ES8+, ES9+ & ES10x Interfaces are for linking the SM-DP+ and eUICC; basically ES8+ interface is used for the profile retrieval from the SM-DP+ down to the eSIM through ES9+ tunnel (between SM-DP+ and LPA) and ES10b tunnel (between LPA and eUICC). Profile operations such as deletion and disabling can be also reported from the eUICC back to the SM-DP+ through the same interfaces.

- ES11, ES12 & ES15 Interfaces are all related to SM-DS. ES11 is used by the device to discover profile availability information and pulls it from the right SM-DP+ accordingly. ES12 is used by SM-DP+ to register an event in the SM-DS for some device. ES15 will be used in case of SM-DS cascading.

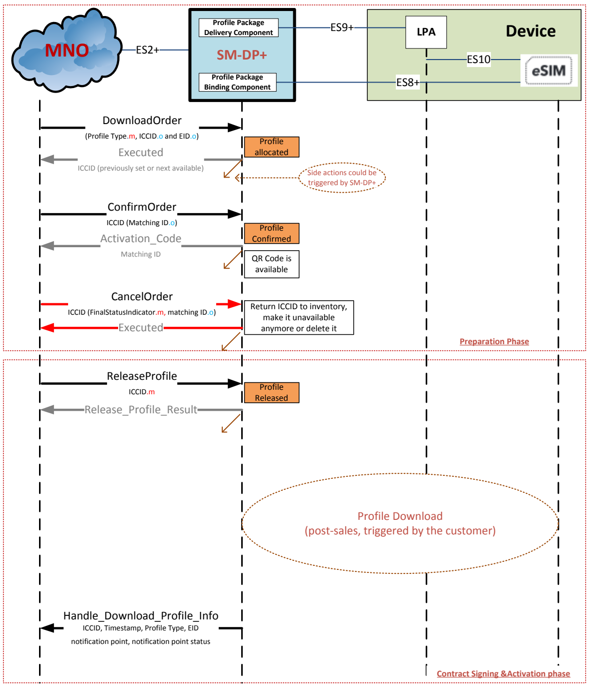
MNO
ES2+
Profile Package Delivery Component
SM-DP+
Profile Package Binding Component
ES9+
LPA
Device
ES10
eSIM
ES8+
DownloadOrder
(Profile Type.m, ICCID.o and EID.o)
Profile allocated
Executed
ICCID (previously set or next available)
Side actions could be triggered by SM-DP+
ConfirmOrder
ICCID (Matching ID.o)
Profile Confirmed
Activation_Code
Matching ID
QR Code is available
CancelOrder
ICCID (FinalStatusIndicator.m, matching ID.o)
Return ICCID to inventory, make it unavailable anymore or delete it
Executed
Preparation Phase
ReleaseProfile
ICCID.m
Profile Released
Release_Profile_Result
Profile Download
(post-sales, triggered by the customer)
Handle_Download_Profile_Info
ICCID, Timestamp, Profile Type, EID
notification point, notification point status
Contract Signing &Activation phase

Fig. 2 ES2+ Interface Commands

- ES6 Interface is used for the traditional OTA (over the air) operations and is not part of GSMA standard for eSIM. Basically it facilitates the usual SIM profile changes that operators used to do, such as changing the SMS Center Address.

C. ES2+ Commands

The following actions can be executed through this interface:

1) Loading SIM profiles on the SM-DP+using the command Download_Order; while this is not mandatory, ICCID is usually known here, EID (Equipment ID) is usually not.

2) Confirming ICCID and extracting the Matching ID (to be used in QR generation or profile retrieval) using the command Confirm_Order; ICCID is known here.

3) Cancelling eSIM order if this is needed after profile is confirmed but not yet released, using the command Cancel_Order. This happens on exceptional basis.

4) Releasing the profile for download using the command Release_Profile.

5) Updating the operator back with the changes happening in the activation (or post-activation) phase using the command Handle_Download_Profile_info

III. DEPLOYMENT, PROVISIONING &ACTIVATION

For MNOs and MVNOs to commercialize their eSIM offering, they have to decide about two main points: (1) how SM-DP+ will be acquired and where it will be located, (2) provisioning and activation options. The first point will involve two options while the second point will involve four options. All of them will be illustrated in this section.

A. SM-DP+ Deployment Options

For MNOs and MVNOs to have SM-DP+ platform and commercialize it, GSMA certificate is a must, which leaves telcos to one of two options:

1) Building GSMA certified data center for SM-DP+

2) Acquiring cloud-based setup from a vendor whose data center is GSMA-certified

As of Q4 2018 when this paper was written, and according to GSMA [7], Telenor's Oslo datacenter is the only fully certified MNO site for subscription manager. Few MNOs and MVNOs such as India's Bharti and UK's Truphone have provisionally certified sites. Two Chinese entities (Eastcomepeace and Wuhan Tianyu) got their Zhuhai data centers provisionally certified as well.

All remaining data centers are owned and operated by the traditional SIM vendors Gemalto, Giesecke &Devrient, Oberthur (Now Idemia) and Valid. Apparently they are still the main players in eSIM and subscription manager domains and it is easier and faster for MNOs and MVNOs to start eSIM by having SM-DP+ as a cloud-based service. With the cloud option, operators should consider three important factors:

- Regulations in the country where the MNO (or MVNO) operates can impact the decision. SM-DP+ does not know MSISDN (mobile station international subscriber directory number) and does not see user information (name, age, etc.), transactions (calls, messages, data) or location, but it knows the IMSI and EID (eUICC Identification).
- Economy of scale should be considered; while eSIM profiles lacks the physical part of traditional SIMs, cost per profile is usually higher than cost per physical SIM; this is because remote SIM provisioning is still new technology and quantities are still limited compared to physical SIM orders; this might not justify the the investment in building local setup and getting it certified. Situation can change in future when it becomes economically efficient for MNOs and MVNOs to invest in building their own local setups.
- Speed of Deployment is quite important and for any MNO or MVNO to build local SM-DP+ and get it certified, it can take quite long time (several months). GSMA released its latest security accreditation scheme for subscription management (SAS-SM) back in March 2017 [8]; the scheme has to be followed by any entity that aims to build its own SM-DP+. On the other hand, having cloud setup from a subscription manager cloud provider can be quite fast (few weeks). In many cases operators need to respond quickly to market dynamics like what happened when Apple launched its iPhone-XS in September 2018 [9]

Should regulatory bodies have no issue, the above points recommend going for the cloud option in the short term and revisiting the idea of building GSMA-certified site when economies change.

B. Provisioning &Activation Options

From provisioning and activation perspective, four main alternatives exist for MNOs and MVNOs, each of which comes with a different depolyment approach:

1) *Pre-printed eSIM Vouchers (Fig. 3)*
2) *On-Demand Vouchers (Fig. 4)*
3) *Entitelement Based Provisioning (Fig. 5)*
4) *Pre-Provisioned Devices (Fig. 6)*

In pre-printed eSIM vouchers, operators get eSIM profiles pre-provisioned on the SM-DP+, associated QR codes, PIN (personal identification number) and PUK (personal unblocking number) pre-printed on paper or plastic cards. Each card (or more precisely QR code) is pre-linked to a downloadable profile on SM-DP+ and is made available in operators' sales stores. With the purchase process, those profiles get associated to MSISDNs in a way that's quite similar to what's happening now with physical SIMs; the eSIM voucher is given to the customer who connects the device to internet–typically through WiFi- and proceeds with eSIM installation by scanning the QR code. In this technique, the three ES2+ interface commands (*Download_Order*, *Confirm_Order* and *Release_Profile*) are effectively pre-executed locally on the SM-DP+ in an offline mode prior to issuing the QR codes. This way does not necessarily need integration between the operator's fulfillment system and SM-DP+, does not need major changes to existing processes, and can work with the standard capabilities of any eSIM enabled device; therefore, it presents the fastest way for MNOs and MVNOs to launch the service. It has the drawbacks of not being that digital as it does maintain the existing SIM logistics practice including paper work and distribution.

In the second option (on-demand vouchers), eSIM profiles are provisioned on the fly at sales points (traditional or online) using the three ES2+ interface commands (*Download_Order*, *Confirm_Order* and *Release_Profile*) and

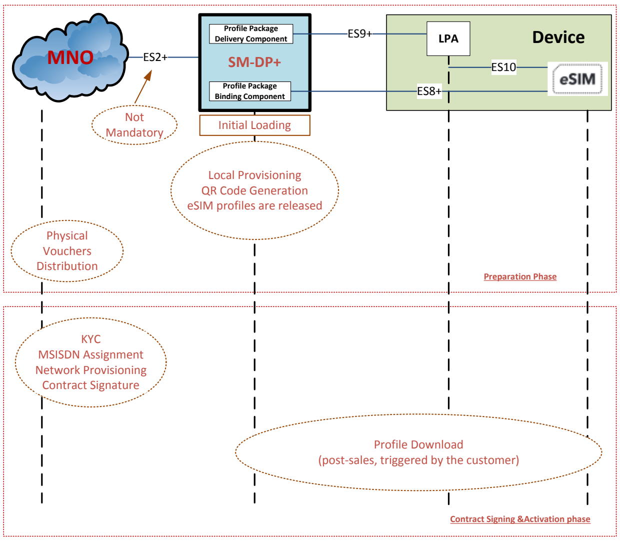
MNO
ES2+
Not Mandatory
Profile Package Delivery Component
SM-DP+
Profile Package Binding Component
Initial Loading
ES9+
LPA
Device
ES10
eSIM
ES8+
Local Provisioning
QR Code Generation
eSIM profiles are released
Physical Vouchers Distribution
Preparation Phase
KYC
MSISDN Assignment
Network Provisioning
Contract Signature
Profile Download
(post-sales, triggered by the customer)
Contract Signing &Activation phase

Fig. 3 Pre-Printed eSIM Vouchers

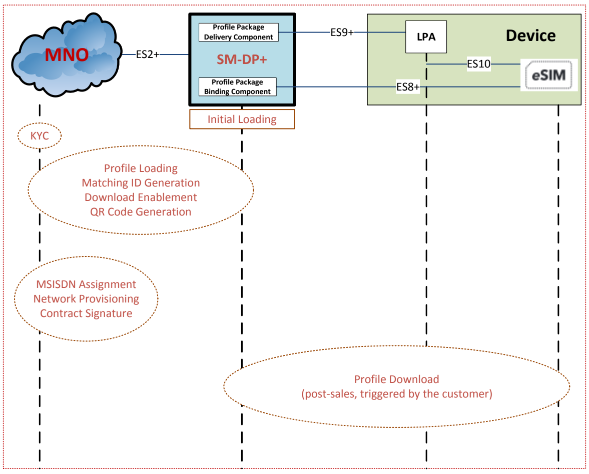

Fig. 4 On-Demand Vouchers

get linked to MSISDNs in the network. QR codes can be sent to users by e-mail. Users can then download the profile using the standard capabilities of any eSIM enabled device. This way needs integration between the operator's fulfilment system and SM-DP+ and therefore it can take some time and efforts; however, it digitizes the SIM handover process and eliminates the usual logistics and paper work associated to physical SIMs; it can also work with the standard capabilities of any eSIM enabled devices and can make SIM purchase process completely online specially in countries where KYC (know your customer) conditions are relaxed or digitized.

In the third option (entitlement based provisioning), MNOs and MVNOs can place an Entitlement Gateway that the device should talk to for activation. The gateway can be programmed to do internal checks (when the information is stored locally on the gateway) as well as external checks with the operator's OSS (operation &support system) and BSS (business support system); it can also do any kind of KYC and digital acknowledgment from the customer. If conditions are passed, the gateway can proxy the provisioning commands the three ES2+ interface commands (*Download_Order*, *Confirm_Order* and *Release_Profile*) to the SM-DP+ prior to eSIM profile download to the device.

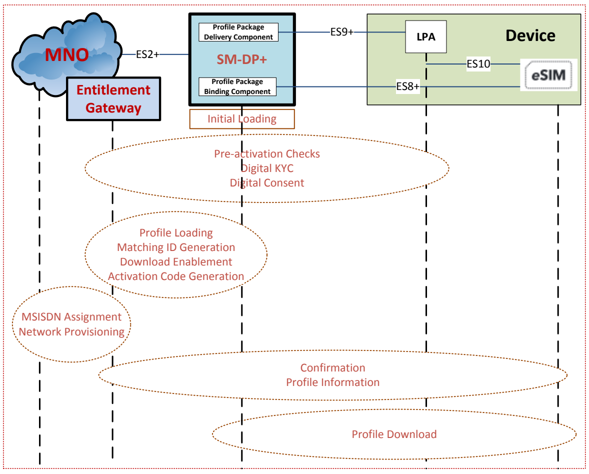

Fig. 5 Entitlement Based Provisioning

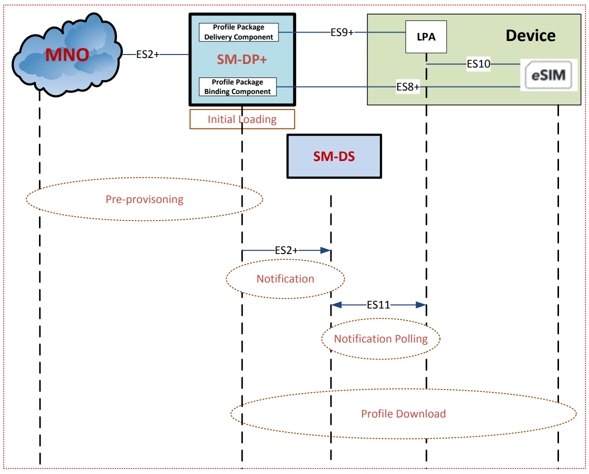

Fig. 6 Pre-Provisioned Devices

While this option has the disadvantages of extra cost for gateway, complex integration and lengthy alignment with device manufacturers, it can digitize the entire customer journey and eliminate the need for customer to use the QR code. Apparently, this approach is being considered by OEM and device operating system vendors [10].

In the fourth option (pre-provisioned devices), there exist two alternatives: SM-DS based pre-provisioning and SM-DP+ based pre-provisioning. In SM-DS based pre-provisioning, operators provision eSIM profiles coupled with pre-identified devices in advance in the SM-DP+; the latter relays this provisioning to a neutral discovery server (SM-DS) that is known in advance to the devices. Once the device is switched on, it automatically interrogates the SM-DS to know is there's an SM-DP+ platform that has an eSIM profile available for it to download and then downloads it accordingly.
In SM-DP+ based pre-provisioning, there's no relay and it's basically the SM-DP+ address that is known in advance to the device. Once the device is switched on, it automatically – interrogates the SM-DP+ for profile retrieval.

This way has the advantage of changing the pull mechanism adopted in eSIM for consumers to a push-like experience where users do not have to manually initiate the download. It has the drawback of being complex in terms of business process as it involves device settings -and possibly subsidizing devices-; also in addition to the integration between operator's fulfillment system and SM-DP+, discovery service based technique requires an integration between the SM-DP+ and the SM-DS. A major concern here is the lack of any known reference implementation following this way as of Q4 2018; in fact, only one SM-DS is fully GSMA certified (Gemalto, Tours) and only one is provisionally certified (Truphone, London). This technique can however be useful in future, especially with consumer IOT devices that are not equipped with rich user interface.

C. *Reflections on customer operations*

- Switching between devices has been irrelevant to MNOs and MVNOs in most of the cases as users can move physical SIMs from a device to another without having to notify the operator; with eSIM, situation is different as movement is technically not possible. Alternatively, operators have to implement a new process in place for this, the process has to involve deprovisioning the old eSIM profile from the mobile network databases such as HSS (Home Subscriber Server), linking a new eSIM profile to the same MSISDN, provisioning the new profile in the network and availing the download of the new eSIM profile to the new device. This is similar to MNOs and MVNOs' existing SIM swap operation (can be called eSIM swap). Depending on operator and regulatory policies, KYC procedure might have to be repeated prior to the eSIM swap.

- Lost or Damaged Device will be treated the same way as switching devices and eSIM swap operation will have to be triggered. KYC procedure will be a prerequisite for triggering this operation.

- Delete Profile option was not available to physical SIM users (they could however get rid of the SIM). With eSIM, users will have the option of deleting their eSIM profiles if they want. Depending on OEM design and on network availability, the device can optionally notify back the SM-DP+ about profile deletion.

IV. eSIM Swap Limitation and Proposed Solutions

A. Limitation

After a successful eSIM profile download, the profile is marked as downloaded in the SM-DP+ and is usually not downloadable again by any other device; users changing their devices for any reason will have to re-download another SIM profile on the new eUICC and operators will have to link the new profile to the same MSISDN in order to maintain the same number purchased by the user. This will have the following disadvantages:

- New ICCID will have to be used, which means that MNOs and MVNOs will have to consume from their repository that is typically purchased from some eSIM solution vendor.

- New HSS profile (IMSI) will have to consumed as well; MNOs and MVNOs usually buy such systems with a specific license that is relevant to number of profiles. If new IMSI means new profile, then there will be a cost fo that.

- Operator's OSS/BSS will have to be triggered for the new process; this is an extra load that MNOs and MVNOs do not have with physical SIMs when users change their handsets for any reason; moving a physical SIM from one device to another does not need operator's OSS or BSS.

While security measurements have to be in place in order to prevent downloading someone's profile in a way or another and having a copy of his/her SIM in an unauthorized way in what is known as SIM cloning [11], this is understood only with stolen or faulty device where the owner does not have an access to the LPA anymore. With a device change, and in the absence of any LPA fault in the old device, there should be a way that users move their profiles from an eUICC to another in a safe way.

B. Proposed Solution

As shown in Fig. 7, proposed solution is about allowing the user to manually transfer eSIM profile from an old device to a new one in a secure way that does not involve new eSIM profile, does not involve new HSS profile and does not require an intevention from the operator.

The following part summarizes the required steps and highlights the newly needed capabilities:

1) User shall use the LPA on the old device (Device-A) in order to to trigger eSim transfer process and provide the EID of the new device (Device-B) to which he/she wants to move the eSIM profile. User interface needs to have this new option.

2) LPA on Device-A shall first ensure SM-DP+ reachability and then take necessary actions to delete the profile from eUICC and notify SM-DP+ using a new command called Transfer_eSIM, with the Device-B information added in this command; this should effectively change the eSIM profile status on SM-DP+ from 'downloaded to Device-A' to 'released to Device-B'. ES8+, ES9+ and ES10 shall have the capability to do those new roles. SM-DP+ can optionally notifies MNO about the status change.

3) The LPA of Device-B shall give the user the option to download a previously transferred eSIM profile; ES8+, ES9+ and ES10 shall have the capability to do this. SM-DP+ shall allow Device-B (and only Device-B) to download the previously transferred eSIM profile and then change its status to 'downloaded to device-B'.

This solution should relief MNOs and MVNOs in case users switch from old devices to new ones while access to old devices is still available. It will also eliminate cost of extra eSIM profiles and extra HSS profiles in their network. What's more, extra OSS/BSS load and KYC checks will be eliminated. It is not applicable however when access to old device LPA is not possible (which can be the case device is completely damaged or stolen). The proposed solution has been submitted to GSMA already and is under consideration.

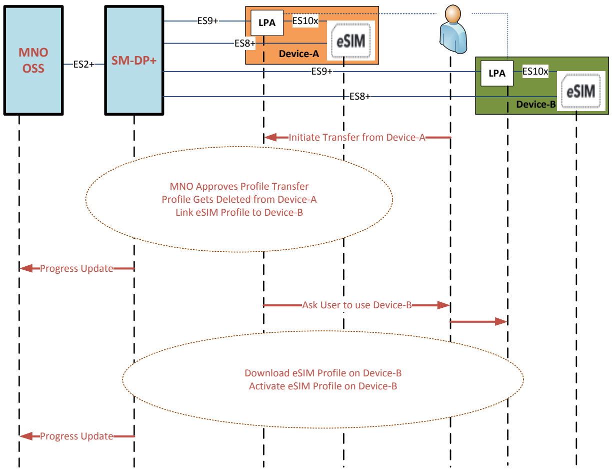
MNO
OSS
ES2+
SM-DP+
ES9+
ES8+
LPA
ES10x
eSIM
Device-A
ES9+
ES8+
LPA
ES10x
eSIM
Device-B
Initiate Transfer from Device-A
MNO Approves Profile Transfer
Profile Gets Deleted from Device-A
Link eSIM Profile to Device-B
Progress Update
Ask User to use Device-B
Download eSIM Profile on Device-B
Activate eSIM Profile on Device-B
Progress Update

Fig. 7 Proposed Profile Transfer Process

REFERENCES

[1] Anonymous, “Understanding SIM Evolution”, GSMA Intelligence, March 2015.

[2] Anonymous, “eSIM white paper, the what and how of Remote SIM Provisioning“, GSMA, March 2018

[3] Anonymous, “RSP Technical Specification Version 2.2“, GSMA, September 2017.

[4] Anonymous, “Remote Provisoning Architecture for Embedded UICC Technical Specification Version 3.2“, GSMA, June 2017

[5] P. Hristova and J. Bryan, “eSIM For The Roaming Consumer,” Roaming Consultancy Company Limited, 2018.

[6] Android Open Source Project (AOSP) Implementing eSIM: https://source.android.com/devices/tech/connect/esim-overview

[7] GSMA SAS-SM Accredited Sites: https://www.gsma.com/aboutus/leadership/committees-and-groups/working-groups/fraud-security-group/security-accreditation-scheme/sas-accredited-sites-list

[8] Anonymous, “GSMA SAS Standard for Subscription Manager Roles Version 3.0“, GSMA, March 2017

[9] Apple Press Release, September 12th: https://www.apple.com/sa/newsroom/2018/09/iphone-xs-and-iphone-xs-max-bring-the-best-and-biggest-displays-to-iphone/

[10] Elite Net Entitlement Server: https://elitenet.eu/products/entitlement-server/

[11] E. Vahidian, “Evolution of the SIM to eSIM,” Norwegian University of Science and Technology, January 2013.