Client-centric on-demand remote profile provisioning technique for M2M IoT Devices

Boheung Chung, Taesung Kim, Keonwoo Kim and Yousung Kang
Cryptography&Authentication Base Technology Research Section
Electronics and Telecommunications Research Institute (ETRI)
Daejeon, South Korea 305-700
bhjung@etri.re.kr

***Abstract*— In this paper, we present a novel approach for client-centered remote profile provisioning that facilitates profile change and selection based on the status of eSIM-equipped devices and customer preferences. By considering the client environment, our proposed method mitigates the occurrence of unnecessary profile changes and eliminates repetitive and time-consuming tasks across multiple devices that arise when using the conventional server-oriented approach. Furthermore, the server-oriented method is unsuitable for seamlessly providing continuous service by immediately replacing devices experiencing errors. In contrast, our provisioning mechanism accurately identifies devices requiring profile changes and efficiently provisions the selected devices. Notably, it offers the advantage of enabling customers to successfully replace their devices at their preferred moment, regardless of factors such as device failure or loss.**

Keywords—RSP, on-demand RSP, Client-centric approach

I. INTRODUCTION

The proliferation of IoT and Machine to Machine (M2M) technology has led to the widespread adoption of diverse wireless access technologies and corresponding services. Consequently, the demand for connecting and managing a vast number of devices has escalated. Traditional approaches rely on subscriber identification modules, commonly referred to as SIM cards, for network registration and device authentication. However, deploying physical card-type SIMs to large-scale IoT devices poses certain challenges. In contrast, eSIM technology offers a promising alternative by being integrated into the device during production, thereby obviating the need for physical SIM replacements [1,2]. Remarkably, eSIMs occupy a significantly smaller footprint than nano-SIM cards, resulting in more compact devices that benefit from enhanced protection against moisture and dust. Moreover, the ability to store and authenticate up to five virtual SIM cards or profiles confers several advantages, including the seamless switching of mobile network operators (carriers) without necessitating physical card replacements or office visits [3].

This study introduces a method for applying profiles to eSIMs through a remote SIM profile provisioning protocol. This involves creating a profile in a remote server, known as the SM-DP (Subscription Manager Data Preparation), and securely downloading/installing it to the eSIM in the target device via a secure communication channel. However, this process typically requires a significant amount of time, often spanning several minutes, to establish and download the profiles through a secure channel. Consequently, this approach may not be viable for selective profile application to specific devices, as it often resorts to bulk installation of subscriber profiles or complete profile changes across all devices, leading to repetitive and time-consuming tasks. Moreover, when a client-oriented necessity arises, such as replacing a malfunctioning device with a new one, the conventional RSP method fails to cater to such scenarios.

This paper presents a client-oriented profile provisioning method designed specifically for M2M IoT devices. The proposed approach enables two-way provisioning, allowing for profiles to be applied at the desired time and according to the device's specific requirements, rather than relying solely on server-centric provisioning that unilaterally progresses without considering client preferences. In order to achieve this, a novel message format is introduced, taking into account the subject and direction of provisioning as well as the necessity for concurrent progress. Additionally, the paper elucidates the process of both server-centered and client-centered provisioning, along with client-centered profile replacement, utilizing the aforementioned message format.

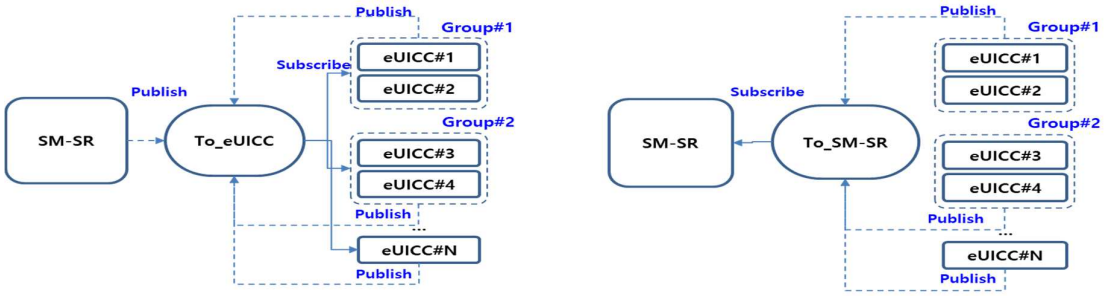
II. BACKGROUND

A. Remote SIM Provisioning

Remote SIM Provisioning (RSP) is a crucial process involving profile change or selection for Subscriber Identity Modules (SIMs), performed over-the-air (OTA). Detailed guidelines for this process can be found in the GSMA's SGP.01/02 document [1,2]. Specifically, the server (SM-DP/SR) modifies/selects the profile for each device's eSIM, following the procedures outlined in the aforementioned document. Provisioning methods can be categorized into two main types: M2M and Consumer methods. In the Consumer method, profile downloads are triggered by the client, while the M2M method triggers profile downloads from the server side [5]. However, in terms of device management, even when employing the M2M method, it is more effective for the client to notify the server regarding the replacement of a faulty device and have a new profile applied based on this information. Furthermore, replacing a malfunctioning device entails substituting a previously used device, making it more efficient to receive and repurpose a profile applied to an existing device rather than generating and downloading a new profile.

B. RSP triggering method and MQTT

The SGP02 standard primarily relies on SMS as the triggering method to initiate RSP. However, emerging low-power wide area networks, such as NB-IoT, which cater to low-end IoT devices, do not inherently support SMS functionality [4]. Consequently, alternative methods need to be employed to address this limitation. Furthermore, it is important to note that SMS is designed to transmit relatively simple data and is not an optimal solution for efficiently delivering medium to large data sets to a small group simultaneously.



Step	Description	Related Topic	Message Format
(A1)	Server-based RSP Trigger Req.	To_eUICC	{nid=0, gid, trigger} or {nid, gid=0, trigger}
(A2)	Result of Server-based RSP Trigger Req.	To_SM-SR	{nid=0, gid, ret(trigger)} or {nid, gid=0, ret(trigger)}
(B1)	Single mode RSP Req.	To_eUICC	{nid, gid=0, msg}
(B2)	Result of Single mode RSP Req.	To_SM-SR	{nid, gid=0, ret(msg)}
(C1)	Multiple mode RSP Req.	To_eUICC	{nid=0, gid, msg}
(C2)	Result of Multiple mode RSP Req.	To_SM-SR	{nid=0, gid, ret(msg)}
(D1)	Client-base RSP Req. #1	To_SM-SR	{nid=0, gid, trigger} or {nid, gid=0, trigger}
(D2)	Result of Client-base RSP Req. #1	To_eUICC	{nid=0, gid, ret(trigger)} or {nid, gid=0, ret(trigger)}
(E1)	Client-base RSP Req. #2	To_eUICC	{nid1, gid, req(nid2)}
(E2)	Result of Client-base RSP Req. #2	To_eUICC	{nid2, gid, profile(nid1)}

Figure 1. Visual representation of the topics and message format used in the detailed steps of the provisioning process

III. On-demand provisioning and Message format

This section elucidates the key considerations pertaining to on-demand provisioning, including the establishment of an MQTT channel for communication between the SM-SR and eUICC. Additionally, it elaborates on the message format employed for seamless exchange of messages within this communication channel.

A. Considerations for on-demand provisionging

The fundamental concept behind on-demand provisioning is to apply provisioning precisely when the target device (eUICC) requires it. However, existing methods typically focus on individual devices and employ one-way message delivery from the server to the client, rather than delivering provisioning precisely at the moment of need. Therefore, in order to effectively realize the core concept, it is essential to modify the delivery method to enable messages to be delivered precisely when they are needed, while also providing a means to accomplish this.

To address this, this research takes into account the characteristics of provisioning initiation and direction diversity, as well as the necessity for simultaneous progress across multiple devices during the provisioning process. The provisioning initiation characteristic involves the provisioning server acting as the initiator and downloading/installing the profile to the target client, as well as the requirement for the client to request the initiation. These characteristics must be considered in the design. The provisioning progress direction characteristic is generally from the server to the client, while the simultaneous processing of multiple devices necessitates a 1:N simultaneous transmission method instead of a conventional server/client 1:1 transmission method to the target device. These aspects need to be reflected in the proposed solution.

Therefore, in this study, the provisioning initiator is categorized into server-centered and client-centered triggering, depending on the entity responsible for initiating the provisioning process. The forwarding direction is divided into the downward direction (from the server to the client), upward direction (from the client to the server), and parallel channel (between clients). Moreover, the need for simultaneous processing of multiple devices is classified as single mode if the profile is delivered to a single device, and multi-transmission mode if it is simultaneously transmitted to multiple devices.

B. MQTT channel and message format

The provisioning procedure typically involves sending a triggering message from the server to the client, establishing a communication channel between them, and then transmitting the message to the client for profile installation. To implement the proposed technique, a new communication channel and message format are established by considering the aforementioned considerations.

In order to enable 1:N message transmission and ensure message quality of service (QoS), an MQTT-based communication channel is created. MQTT allows the sender to write to a topic and the receiver to read from the topic, so the number of topics to be set needs to be determined. Since the forwarding direction supports only upward, downward, and parallel channels, it is sufficient to create two topics: 'To_SM-SR' as the server topic and 'To_eUICC' as the client topic, based on the destination. The transmission mode needs to be considered only when the provisioning characteristic is in the client direction. With two topics focused on the destination, the message format is designed to express single or multiple transmission modes.

The provisioning process message contains the triggering message request/result, command message requests/results related to provisioning, target device information, and transmission mode. For single destination transmission, devices are identified by a unique ID. In the case of multiple destination transmission, devices are grouped with the same ID. The message format {'nid', 'gid', 'type', 'body'} includes device ID, group ID, message type, and content. 'nid' represents the individual eUICC identifier, while 'gid' represents the eUICC group identifier. Non-zero values for 'nid' and 'gid' indicate multiple transmission mode, while 'nid' being non-zero and 'gid' being zero indicate single

transmission mode. The 'type' field can have values such as {'trigger' | 'msg' | 'ret(trigger)' | 'ret(msg)' | 'req(nid)' | 'profile(nid)'}. 'trigger' and 'ret(trigger)' are for triggering message request and response, while 'msg' and 'ret(msg)' are for provisioning command message request and response. 'req(nid)' and 'profile(nid)' are values for response. Detailed specifications for 'msg', 'trigger', and 'ret' adhere to the GSMA RSP standard for device authentication and transmission data protection.

IV. Implementation of Bi-directional, On-demand Provisioning

A. Preliminary procedures and provisioning processes

To facilitate the proposed provisioning process, it is crucial to establish a communication channel between the SM-SR and eUICC through a preliminary setup procedure. This involves creating two topics, namely 'To_eUICC' and 'To_SM-SR', as illustrated in Figure 1. The SM-SR and eUICC establish a publish/subscribe relationship for these topics. Furthermore, a group identifier (gid) is assigned to eUICCs that belong to the same group, and this gid is shared between the SM-SR and the corresponding eUICCs.

Subsequently, the provisioning process unfolds through triggering message transmission and provisioning command message execution. Taking into account the MQTT channel, topics, message structure, and the proposed technique's characteristics such as server-centric or client-centric approaches and single or multiple transmission modes, the detailed steps can be categorized as follows:

(A) Server-centric triggering: (A1), (A2)

(B) Perform single-mode provisioning: (B1), (B2)

(C) Perform multi-mode provisioning: (C1), (C2)

(D) Client-centric triggering: (D1), (D2)

(E) Replacing client-centric profiles: (E1), (E2)

B. Server-centric provisioning

The server-centered provisioning process involves the SM-SR initiating a triggering message towards the eUICC, followed by provisioning command execution in steps (C). In contrast to the existing provisioning method, which requires repeating steps (A) to (B) for each device in multi-device scenarios, the proposed method simplifies the process by performing steps (A) to (C) only once. This approach offers a more efficient and streamlined provisioning procedure.

C. Client-centric provisioning

The newly introduced client-centric provisioning process follows a flow where the eUICC sends a triggering message towards the SM-SR and performs a provisioning command. In terms of mode, it proceeds in the order of (D) -> (A) -> (C). With this method, the client-side notifies the server of the provisioning requirement and subsequently executes the existing provisioning process, allowing provisioning to be performed on the desired target at the desired moment. This approach proves particularly effective when adding a new eUICC, as it enables quick provisioning to the correct device at the precise moment, ensuring service continuity and security without the need for immediate service restart upon server-side recognition of the demand and RSP triggering message transmission using the existing provisioning method.

D. Client-centric profile replacement

The client-centric profile replacement process involves the eUICC initiating a profile replacement request towards another device and receiving the corresponding profile, following the sequence (E1) -> (E2). However, in contrast to the existing server-centric/client-centric provisioning approach, message and profile delivery occurs through sharing the 'To_eUICC' topic, obviating the need for two separate topics. Both the device sending the profile and the device receiving it simultaneously publish/subscribe to the 'To_eUICC' topic. Subsequently, in step (E1), when the new device (nid2) sends a {nid, gid, req(ni2)} message to the device being replaced (nid1), the device being replaced responds in step (E2) with {nid2, gid, profile(nid1)}. This scenario assumes the reuse of an existing profile during device replacement and is only feasible when both devices adhere to the same pre-agreed system environment and operating conditions. In cases where this condition is not met, a new device should be added, and client provisioning should be performed to replace the profile.

V. Conclusions

In conclusion, this paper presented a client-centered remote profile provisioning approach, which effectively facilitates profile change and selection based on the status of eSIM-equipped devices and customer preferences. The proposed method ensures service continuity and security by enabling the application of a new profile to a desired device at a desired time through bi-directional provisioning, considering the provisioning subject and direction. Moreover, simultaneous transmission was employed to address the need for concurrent progress, resulting in enhanced efficiency for profile application by eliminating time-consuming and repetitive processes when installing profiles on multiple devices simultaneously. Future research should focus on evaluation of proposed scheme and investigating the applicability of the proposed provisioning method to larger-scale deployments and mobile objects such as drones, thereby further expanding its potential benefits and practical implications.

Acknowledgment

This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No.2022-0-01019, Development of eSIM security platform technology for edge devices to expand the eSIM ecosystem)

References

[1] "Embedded SIM Remote Provisioning Architecture", GSMA, June 2020.

[2] "Remote Provisioning Architecture for Embbedded UICC", GSMA, July 2020.

[3] Abdou and Bassem Ali, "Commercializing eSIM for network operators.," 2019 IEEE 5th World Forum on Internet of Things (WF-IoT). IEEE, 2019, pp.616-621.

[4] Ken-Tristan Peterson(2020), M2M embedded subscriber identity module provisioning in networks without SMS service [Master's thesis, TALLINN UNIVERSITY OF TECHNOLOGY], online available.

[5] Apilo, Olli, Pekka Karhula, and Jukka Mäkelä, "eSIM-Based Inter-Operator Mobility for Advanced Smart Products.," IEEE Internet of Things Magazine 5.2 (2022): pp.120-126.