AKMA Support in Multi SIM User Equipment

Gizem Akman, Valtteri Niemi
University of Helsinki, and
Helsinki Institute for Information Technology (HIIT)
Helsinki, Finland
gizem.akman, valtteri.niemi@helsinki.fi

Philip Ginzboorg
Huawei Technologies, and
Aalto University
Helsinki, Finland
philip.ginzboorg@huawei.com

***Abstract*— Multi SIM User Equipment (UE) can have more than one physical slot for Universal Integrated Circuit Card (UICC). The eUICC is an embedded version of the UICC, which cannot be physically removed from the communication device. Currently, 3rd Generation Partnership Project (3GPP) is working on developing Authentication and Key Management for Applications (AKMA), with which user can bootstrap authentication towards application server from his mobile subscription. We consider the scenario that may become common in devices with Multi SIM and eUICC, in which one subscription is used for primary services such as voice and data, and another subscription is used for AKMA services. In this scenario, the purpose is to use AKMA services simultaneously and without interrupting primary services. There are existing requirements for Multi SIM and eUICC, which restrain this scenario from being successful. The solution that we propose includes arrangements and adaptations, in order to provide secure and uninterrupted services of both primary and AKMA services.**

I. INTRODUCTION

Dual SIM phones have two physical slots for inserting the Universal Integrated Circuit Card (UICC). To the consumer they offer the advantage of increased convenience and reduced costs by being able to access different mobile networks from a single smart phone based on, e.g., price or signal strength. In addition, phones that can use more than two physical UICCs have been produced [1], [2]. Dual SIM phones have one or two transceivers. The variety in the number of transceivers and the way in which radio connection via a transceiver is multiplexed, creates different modes of Dual SIM devices. One of those modes is Dual SIM Single Standby (DSSS), where the device has one transceiver through which it can have one radio connection. Another mode is Dual SIM Dual Standby (DSDS), where the device has one transceiver, but two radio connections through that transceiver are possible by using time multiplexing techniques. Third mode is Dual SIM Dual Active (DSDA), where a device has two transceivers, and so can have two radio connections simultaneously [3], [4]. In case that more than two Universal Subscriber Identity Module (USIM)s exist in the smart phone, hybrid modes can appear [4].

Standardization of Multi SIM devices has taken off in GSM Association (GSMA), European Telecommunications Standards Institute (ETSI) and recently 3rd Generation Partnership Project (3GPP). The GSMA has produced requirements for Multi SIM devices [4]. The 3GPP services working group SA1 has completed a study of Multi SIM requirements and use cases [5]; it now has a work item on this topic [6], [7]. In addition, the study of Multi SIM devices has been proposed in 3GPP RAN group [3].

Another relatively recent development is the standardization of Embedded Universal Integrated Circuit Card (eUICC) in ETSI and GSMA. The eUICC is an embedded UICC in a communication device that can be managed remotely without physical removal or replacement of the UICC [8]. Remote SIM Provisioning (RSP) is combination of downloading, installing, enabling, disabling, switching, and deleting of a Profile on an eUICC [9] and the Profile in the eUICC is a combination of all data related to the subscription, which is necessary for providing services. According to GSMA, the content and structure for interoperable Profiles stored on eUICCs are similar to those installed on traditional SIMs [10]. The use case envisioned for eUICC include both Machine-to-Machine (M2M) [11] and consumer devices [12].

We expect that Multi SIM phones in the future will be based on the eUICC technology, instead of having several physical UICCs [13].

Currently, 3GPP is studying Authentication and Key Management for Applications (AKMA) service that is being developed for 5G authentication architecture [14]. It is essentially a key distribution service, where the authentication can be bootstrapped towards application server from mobile subscription of the user. The standardization of AKMA is still in early stages, and it is not yet clear if the resulting standard will support interoperability of AKMA between operators. Even if it would, interoperability of AKMA service between operators will take time to emerge.

In this paper, we are concerned with a situation where a user has a Multi SIM phone with one USIM used for voice and data service and another USIM for AKMA service. For example, there is a user, who has a main subscription for voice and data with one Mobile Network Operator (MNO), but he/she wants to use a service that is accessible via AKMA to subscribers of another MNO. For instance, the user may have a connected car where some functions of the car can be controlled via an application on a smart phone. The user needs to utilize AKMA in order to start using the application. While doing these, the user may need to use voice services on main subscription. In this situation, it is required that both voice (provided by one subscription) and AKMA service (provided by another subscription) can be used at the same time.

Double-transceiver phones are suitable for our scenario, if there are only two USIMs and one of these USIMs is used for AKMA. If there is a need for one more USIM for AKMA, then also double transceivers are not enough.

ISSN 2305-7254

We expect that most Multi SIM phones will have a single transceiver, because an additional transceiver in double-transceiver phone makes the phone more expensive.

A single-transceiver, Dual SIM phone having only dual passive mode is not useful for our scenario, because with such phone USIM1-AKMA and USIM2-voice cannot be used simultaneously. A dual standby mode phone may be more suitable for our scenario. However, there may be a problem in this mode, if the phone does not retain session information when the USIM-AKMA is in the standby state.

We observe that the requirements of eUICC architecture include the following: “the behavior of the eUICC with an Enabled Profile shall be equivalent to the UICC”, and “at a maximum, only one Profile shall be enabled at any point in time” [9]. Because of these requirements, we can say that the phone with eUICC acts like a dual-passive device. Thus, our scenario will not work with a phone having eUICC.

We propose a solution to this problem by combining several solutions for AKMA proposed in the 3GPP technical report [14] and adapting them to eUICC and Multi SIM architectures. By this configuration, we aim to perform AKMA authentication in a secure way without interrupting services from primary subscription.

II. Background

This section briefly explains the technical details that are needed for this paper. We start with the definitions of fundamental elements, which are important for the rest of the paper. Then, we provide technical details and explanations of Multi SIM, eUICC, and AKMA. Our argument is based on these elements.

A. Definitions

SIM (Subscriber Identity Module) is the physical entity that contains keys and ID that are required for authenticating the user to a mobile network.

UICC (Universal Integrated Circuit Card) is the physical entity that contains the SIM/USIM application.

UE (User Equipment) is the user's mobile device in 3G, LTE and 5G cellular networks. For the purpose of this paper, the UE can be thought of as having two main parts: (i) the UICC, and (ii) the Mobile Equipment (ME) part that includes the rest of the UE.

USIM (Universal Subscriber Identity Module) is an application that runs on the UICC and provides authentication functions similar to those provided by the SIM in pre-3G systems.

eUICC (Embedded Universal Integrated Circuit Card) is an embedded UICC in a communication device. The eUICC can be managed without physical removal or replacement of the UICC. The eUICC contains USIM application(s), similarly as UICC does.

Profile is a specific SIM/USIM application contained within an eUICC.

B. Multi SIM

The current technology allows simultaneous access of more than two USIMs from a single device to the mobile network services [15]. Changing between subscriptions happens easier than with single SIM devices, in the way that for Multi SIM devices, several UICCs can be stored in the device simultaneously and changing between subscriptions would not require changing UICCs physically. This property is very helpful for customers who would like to always choose the cheapest option for every different service or who are in some locations with unstable coverage. The latter case can be eased by connecting to two (or more) networks [16].

When two UICCs are allowed in mobile devices, these are called Dual SIM devices. If two or more UICCs are allowed in mobile devices, then these are called Multi SIM devices [4]. One of the market studies reveals that one out of three smart phones sold globally is a Dual SIM Dual Standby (DSDS) device [17]. The DSDS UE, explained below, seems to be favored by both customers and manufacturers.

In the specification document of GSMA [4] and working group meetings of 3GPP [3], the different operation modes of Multi SIM devices are explained. These specifications and studies consider mostly the Dual SIM cases, but implementations with more than two USIMs are not excluded. Fig. 1 displays state combinations for different modes of Dual SIM, which we explain below;

1) Dual SIM Single Standby (DSSS), also can be named as Passive Dual SIM [4], has two UICC slots, but it has only one transceiver, which can provide only one logical connection to one network at a time. Therefore, only one of the USIMs can be chosen and be active.

2) Dual SIM Dual Standby (DSDS) devices share one transceiver, similarly to the DSSS devices. However, by using time multiplexing two radio connections can be provided when the both USIMs are in idle mode. When one of the USIMs is activated, the other USIM loses the connection, but its registration for the network is maintained.

3) Dual SIM Dual Active (DSDA) devices contain two transceivers. Therefore, both USIMs can be active both in idle and connected modes; they act independently with respect to the other USIMs activity.

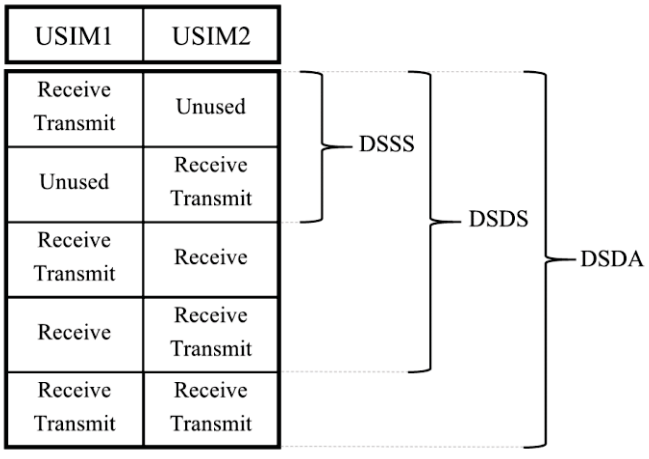

Fig. 1. State combinations in different Dual SIM modes

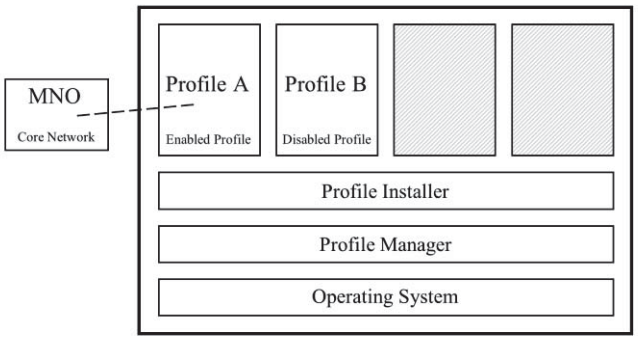

Fig. 2. eUICC architecture; adapted from [8]

Besides Dual SIM cases, Multi SIM cases are also possible in mobile devices.

C. eUICC

Embedded UICC (eUICC) stores Profiles and allows remote management of the Profile over-the-air. There can be zero or more Profiles in the eUICC [9]; the maximum number Profiles depends on the capacity of eUICC [10]. A schematic illustration of eUICC Architecture is shown in Fig. 2. As shown in the figure, only enabled profile has connection with MNO core network. The gray Profile slots indicate empty slots for Profiles which can be downloaded in the future. Profile Installer and Profile Manager are elements in eUICC that are in contact with elements of MNO. These elements are responsible for downloading, storing, enabling, disabling, deleting, and updating of Profiles in the eUICC [10].

According to one eUICC requirement, eUICC shall provide isolation of data and applications between Profiles [8]. Content of eUICC cannot be reached and applications in eUICC cannot be triggered, unless the Profile is active [12].

Profiles stored in the eUICC have two different statuses: enabled and disabled. The eUICC with enabled Profile is expected to behave like a regular UICC [12] and it provides connection with the mobile network. On the other hand, when the Profile is disabled it stays installed in eUICC, but applications in the Profile cannot be selected and the files in the Profile cannot be reached by the device or by any application on eUICC [8].

One of the eUICC requirements of GSMA, EUICC5, states that at the maximum, only one Profile shall be enabled at any point in time [9]. So, if the user enables Profile B, while Profile A was active, Profile A becomes disabled immediately before Profile B can be active.

The specifications do not explain reasons of the restriction for having at most one active profile. One reason for this requirement could be that the behavior of eUICC was wanted to mimic the traditional setting of a UE with one slot for a removable UICC, as closely as possible. Now changing of active profile corresponds to change of physical UICC in the traditional UE.

In Fig. 3, we show flow of messages related to eUICC, based on GSMA publications [9], [10], [18]. The messages, which are presented in the figure, are sent during the communication between UE and different networks, while user changes Profiles

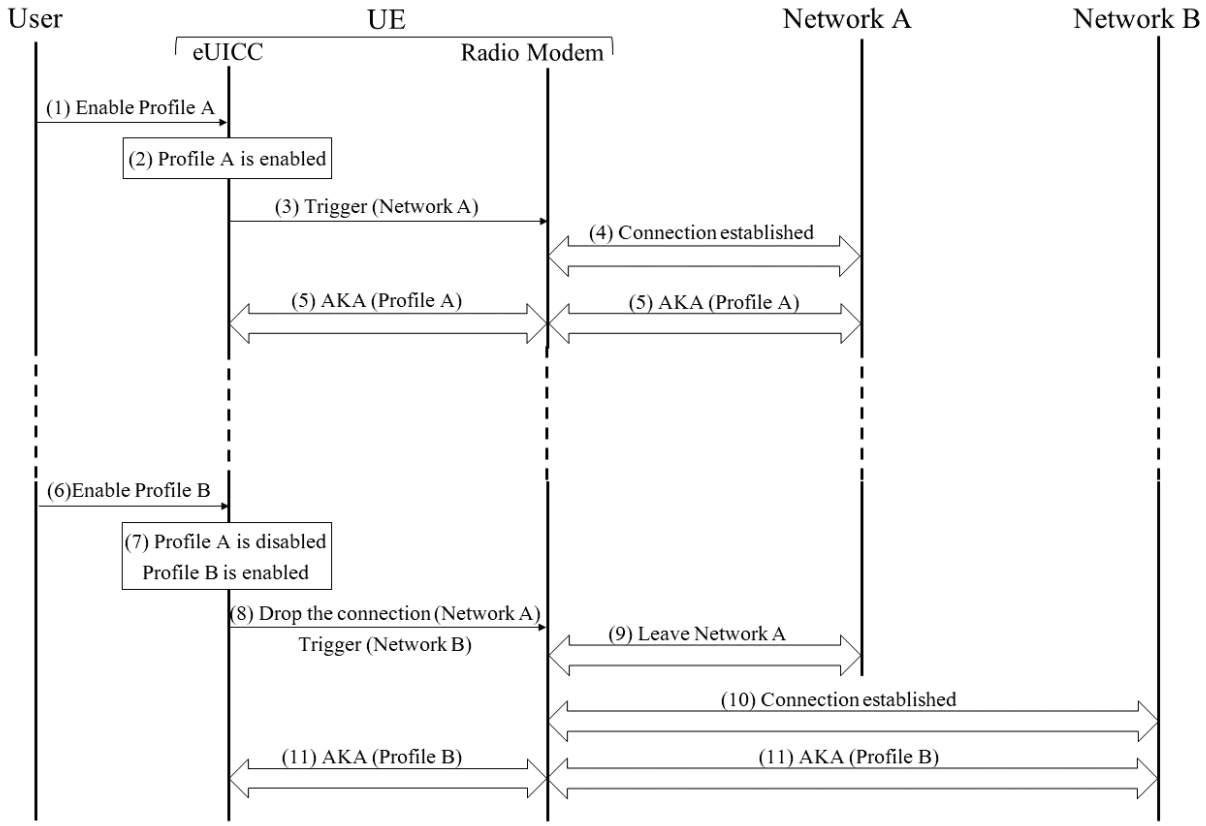

Fig. 3. Flow of messages related to eUICC

in eUICC. The numbers on Fig. 3 correspond with the numbers below. Network A and Network B denote the networks, associated with Profile A and Profile B, respectively.

In the beginning of Fig. 3, we assume that Profile A has been downloaded to eUICC recently and it is the only Profile on eUICC.

1) User wants to enable Profile A.

2) Profile A is enabled in eUICC.

3) The eUICC sends request to Radio Modem for triggering Network A to establish connection.

4) Connection is established between UE and Network A.

5) After the connection is established, Authentication and Key Agreement (AKA) procedure is initiated between Profile A and Network A. If the AKA is successfully completed, then User can start using services with Profile A.

Note: After the Step (5), User continues using Profile A. In this stage, many other Profiles might have been downloaded to the device. This does not have effect on the services of Profile A, until one of those Profiles is enabled.

6) User wants to enable another Profile, Profile B.

7) The eUICC disables Profile A, and then enables Profile B.

8) The eUICC requests Radio Modem to drop the connection between Profile A and Network A, and triggers connection to Network B.

9) Radio Modem informs Network A that Profile A left the network.

10) After leaving Network A, Radio Modem establishes connection with Network B.

11) After the connection is established, AKA procedure is initiated between Profile B in the eUICC and Network B. If the AKA procedure is successfully completed, then User can start using services with Profile B.

With every Profile, which is enabled while another Profile is active, steps 6-11 of Fig. 3 will be repeated.

D. AKMA

Since the 3GPP authentication infrastructure and 3GPP AKA procedure are considered as valuable assets for 3GPP operators, 3GPP has standardized Generic Bootstrapping Architecture (GBA). It is a mobile network service for bootstrapping of application security based on AKA procedure in Evolved Packet System / Universal Mobile Telecommunications System (EPS/UMTS) [19]. In essence, GBA is a key distribution service for applications, where the session key between UE and application server is bootstrapped from AKA.

3GPP is currently studying a similar service, called Authentication and Key Management for Applications (AKMA), for 5G system [14]. The AKMA architecture includes two new network functions. These functions are AKMA Authentication Function (AAuF) and AKMA Application Function (AApF). AKMA Application Function uses the authentication service of AAuF and gets the key for the secure channel. AKMA authentication function is responsible for authenticating UE and managing the key material related to UE.

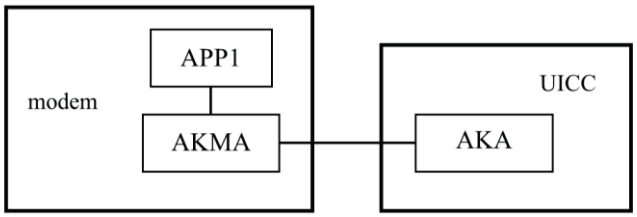

Fig. 4. AKMA framework and UICC; adapted from [2]

The AKMA study of 3GPP, in TR 33.835 [14], contains several potential solutions for various important problems. Next, three of these proposed solutions for AKMA are explained. These solutions are referred by the numbers from [14] while constructing our proposal. Following [14], the term "AKMA framework" denotes the AKMA module in the mobile equipment – the part of the UE that includes the application processor and the radio modem but does not include the UICC.

1) AKMA Solution 7: "UE implementation scheme – AKMA framework and application on modem".

In this solution, AKMA framework and the applications are implemented on modem. 3GPP AKA runs on UICC. The Cipher Key and the Integrity Key (CK and IK), which are obtained from 3GPP AKA, are given to AKMA framework to be used in deriving session key for AKMA. The AKMA framework requests these keys via Application Protocol Data Units (APDU) messages. Along with these keys, some other parameters including identifiers can be exchanged between AKMA framework and UICC. Fig. 4 presents the relation of the AKMA framework and the UICC.

2) AKMA Solution 13: "AKMA authentication via the control plane".

The purpose of this solution is to perform independent AKMA authentication, without repeating primary authentication, to obtain K_{AKMA}, which is the AKMA-specific key that is derived based on the AKA procedure. In Fig. 5, the AKMA reference architecture is shown.

When UE and AApF agree to have a secure communication, UE starts AKMA authentication with AAuF. In the end of authentication, both UE and AAuF have a key, K_{AKMA}. Then, UE generates a new key, K_{AF}, by using some parameters, including the identifier of AApF. The AAuF generates the K_{AF}, when AApF requests the key information related to UE. Then, AAuF provides the K_{AF} to AApF.

3) AKMA Solution 15: "Implicit Bootstrapping".

The AKAF is AKMA Anchor Function, which can be same as Authentication Server Function (AUSF) or a separate entity. This solution is about refreshing the AKMA Anchor key, K_{AKMA}, without repeating primary authentication in UE and AKAF. The solution offers two options for the derivation of K_{AKMA}, one is as a sibling and other is as a child key in relation

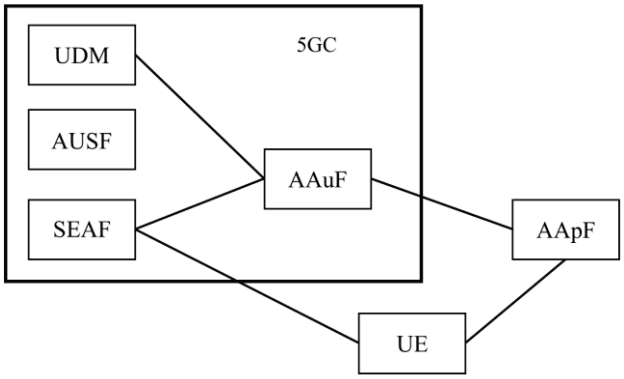

Fig. 5. AKMA reference architecture; adapted from [2]

to K_{AUSF}. In case of AKMA key refreshing, sibling keys require primary authentication in order to get new K_{AKMA}. On the other hand, if K_{AKMA} is derived from K_{AUSF}, a freshness parameter, such as a sequence number that is held by AKAF/AUSF, can be included during the derivation. This refresh procedure can be used for both options of primary authentication in 5G system, EAP-AKA' and 5G AKA. When it is needed to refresh the K_{AKMA}, AKAF obtains freshness parameter from AUSF and sends it to UE. The visualized version of the key hierarchy for deriving K_{AKMA} as a child key is presented in Fig. 6.

The UE sends the request for AKMA authentication to Core Access and Management Function/Security Anchor Function (AMF/SEAF) over Non-Access Stratum (NAS) and they recognize the request for the AKMA authentication and forward the request to the correct home network entity, AAuF. Then, AAuF gets AV from Unified Data Management (UDM) and learns the authentication method. Between AAuF and UE, either 5G AKA or EAP-AKA' is performed for AKMA purposes. If the authentication ends successfully, AAuF and UE have fresh K_{AKMA}.

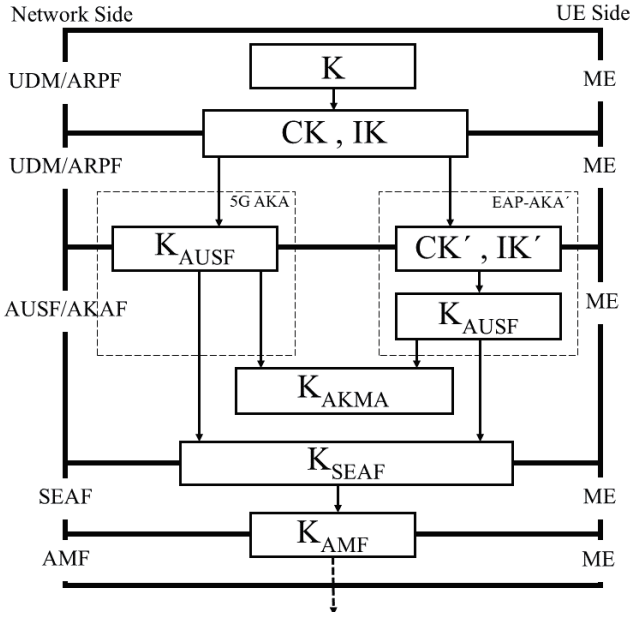

Fig. 6. Key Hierarchy for K_{AKMA}; adapted from [2]

III. Multi SIM and eUICC standardization

The GSMA has technical specification for Multi SIM, the recent version was published in December 2018 [4]. GSMA and ETSI have technical specifications about eUICC. The technical specification from ETSI is TS 103 383 [8] and the latest version was published in July 2018. GSMA has been working on eUICC, while developing RSP. Different technical specifications were published for Machine-to-Machine devices and consumer devices, in terms of RSP technologies. These papers, SGP.01 [18] and SGP.02 [11], are about RSP architecture for eUICC in Machine-to-Machine devices. SGP.21 [9] is about RSP architecture and SGP.22 [12] is technical specification about RSP in consumer devices with eUICC.

Multi SIM has been discussed in working groups of 3GPP. According to the Work Item Description with number SP-190309, "SA1 WG has started the study for use cases, concluded and identified consolidate potential service requirements in TR 22.834, which is ready for sending SA Plenary's approval" [6]. With Stage 1 technical specifications and requirements, it will be easier to improve and contribute to Multi SIM devices for Evolved Packet System (EPS) and 5G. Short after the above claim in SP-190309, 3GPP published the technical report about Multi SIM devices [5]. In this technical report and other 3GPP documents, Multi SIM is referred as Multi USIM and abbreviation is used as MUSIM. Uses cases related to Multi USIM Devices are published in TR 22.834 [5].

IV. Problem statement

Implementing more than one USIM per mobile device gives users opportunities for preferring different MNOs for different services.

If the user prefers a particular MNO for his/her voice and data services (primary subscription), but another MNO offers a more attractive AKMA service, then the user can decide to put an extra USIM for AKMA to a Multi SIM device or download an extra Profile to eUICC. Therefore, we are interested in scenarios for Multi SIM device usage, where USIM1 of one MNO is used, e.g., for voice, data, and USIM2 of another MNO is used for AKMA. With this scenario, the purpose is executing AKMA with USIM2 without interrupting the services on USIM1. Please note that this scenario can be extended to multiple USIMs from different MNOs used for AKMA. If many services start using AKMA, then there might be multiple MNO requirements for user. Each service might have agreements with different MNOs. If the user wants to use these services, he/she should have subscriptions from related MNOs. Then, if the user starts using several services one after another, changing between USIMs would be too time consuming and inefficient.

When the different modes of Dual SIM are considered, DSSS will not support the scenario. Two USIMs cannot be active at the same time. Therefore, it is not possible to use AKMA services with USIM2 without interrupting the services with USIM1. The other mode, DSDS, could support the scenario with certain provisions. When USIM1 is in idle mode, USIM2 can perform AKMA. However, when USIM1 is active,

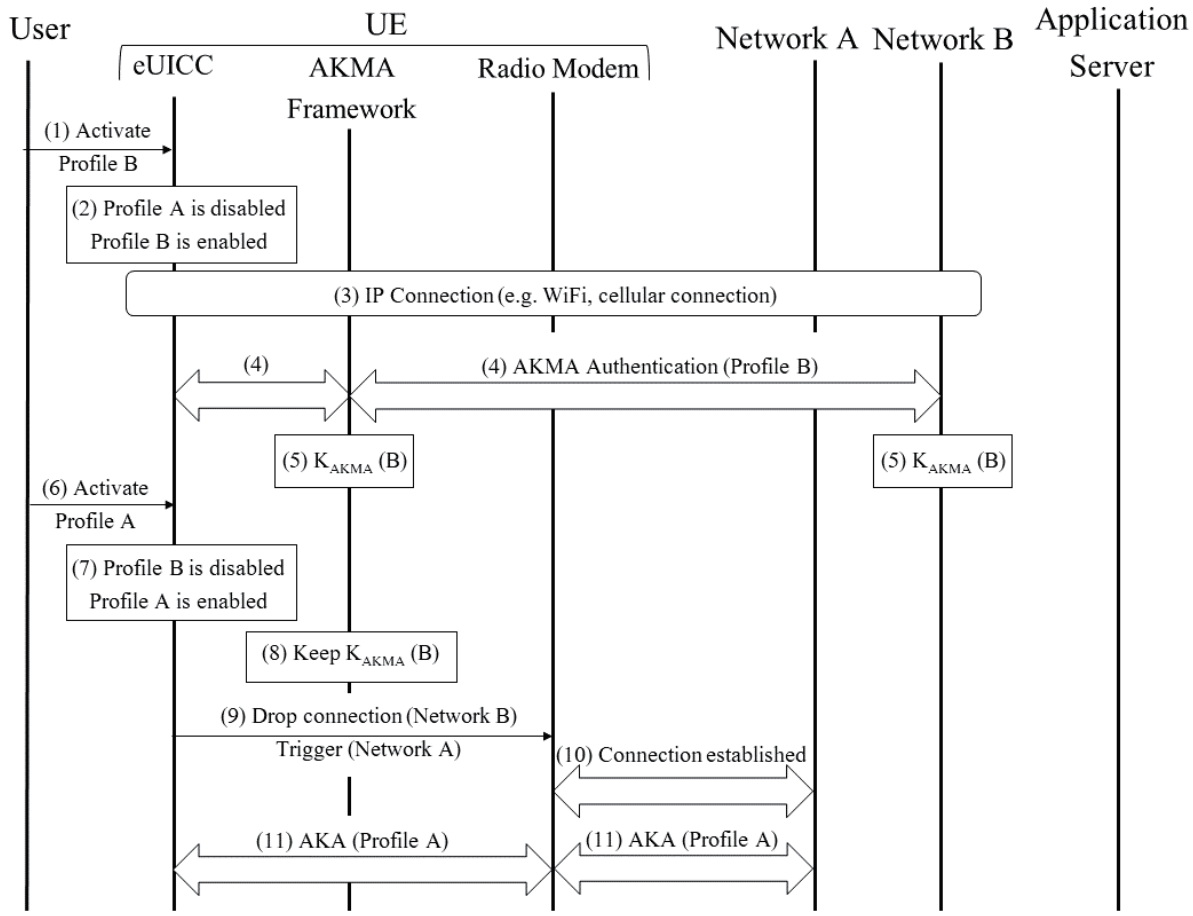

Fig. 7. Flow of relevant messages for solution case of eUICC

the radio connection of USIM2 is lost. Another mode is DSDA and this mode would support the scenario. The problem of this mode is that DSDA mode needs two transceivers (radio modems) in the mobile equipment, which increases the cost of device.

It is possible that Multi SIM phones will be based on the eUICC technology, rather than on many physical UICCs, in the future. In case of the scenario considered in this paper, the eUICC would not support it. Unless a Profile is enabled, the eUICC acts like this Profile does not exist. However, if this Profile is enabled, the active primary Profile is disabled automatically, and all the services are interrupted [8]. Even though AKMA does not require radio connection, it does not function efficiently with the scenario.

In addition to mobile services, such as data, voice, Short Message Service (SMS), and Multimedia Messaging Service (MMS), AKMA authentication shall be considered as one of the mobile services. Users should have eligibility to choose the operator for completing AKMA authentication. However, AKMA authentication should not interrupt the connection of other active services.

It could be noted that, independently of AKMA, it would make sense to provide a Multi SIM functionality in a device having just one eUICC (that is, a device without a physical UICC).

V. SOLUTION

Assume that a smartphone has eUICC with two profiles or it is Multi SIM phone with two USIMs. Profile A (USIM A) is for primary use, such as data connection, phone calls, etc. Profile B (USIM B) is for AKMA authentication for a service, such as an application or an online platform. According to the eUICC architecture specification, Profile A needs to be disabled in order to AKMA authentication to be completed with Profile B [9]. Disabling Profile A means that the data connection would be lost, and phone calls would be interrupted.

Our purpose is to complete AKMA authentication for Profile B without interrupting the connection of Profile A.

In the rest of the section, possible AKMA solutions for eUICC and different operation modes of Multi SIM are explained.

A. Case of eUICC

In the beginning of the solution for eUICC case, we assume that the primary profile, Profile A, is enabled. User enables Profile B, when he/she is not actively using Profile A. This process can be done early in the morning or can be triggered automatically during nighttime. The frequency of repeating the following procedure depends on the lifetime of the key. This procedure is summarized in Fig. 7 and numbers on the figure correspond to those below. Network A and Network B denote the networks associated with Profile A and Profile B, respectively.

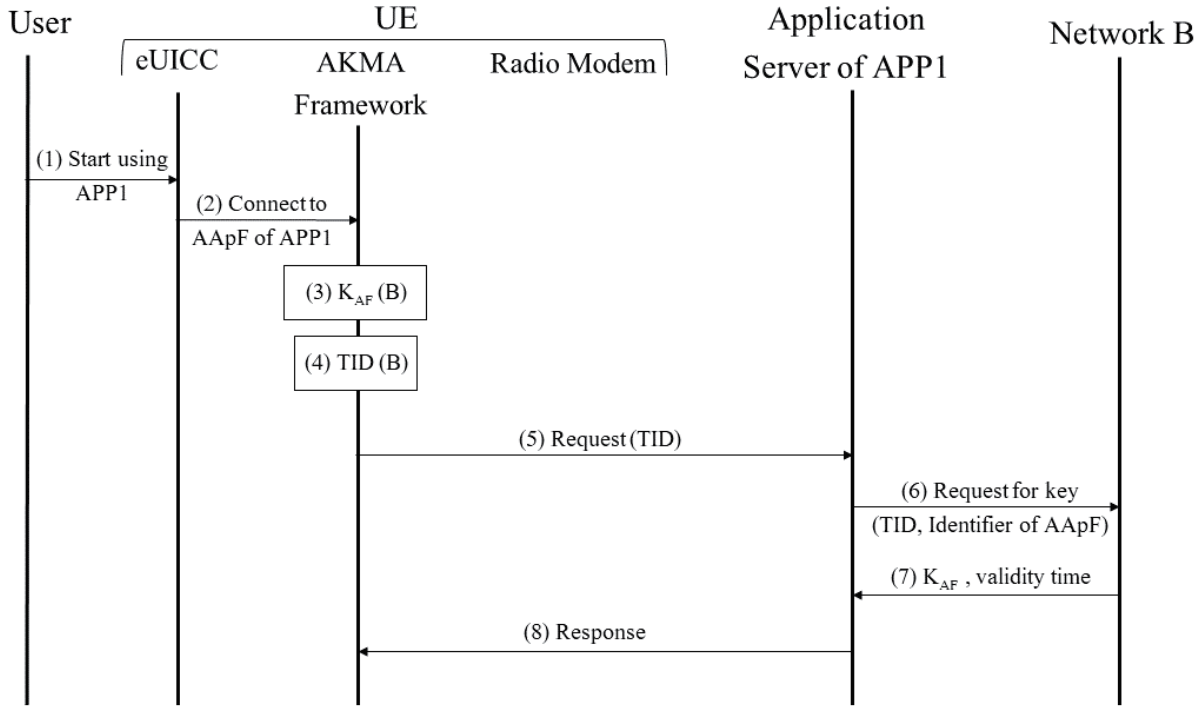

Fig. 8. Flow of relevant messages continues from Fig. 7

1) User wants to enable Profile B to perform AKMA authentication and to store its product, K_{AKMA}.

2) When the User gives the command for enabling Profile B, the Profile A becomes disabled immediately [8]. After the Profile A is disabled, then Profile B becomes enabled.

3) In order to continue, an IP connection, such as cellular connection of Profile B, e.g. the steps 8 to 11 from Fig. 3 with additional steps to establish IP connection from UE to AAuF in network B, or WiFi connection, should be established.

4) When the Profile B is enabled and IP connection is established, AKMA authentication between Profile B and Network B takes place through AKMA framework.

5) If the authentication is successful, a key, K_{AUSF}, is derived as explained in the Solution 4 of 3GPP TR 33.835 [14]. Then, K_{AKMA} is derived from K_{AUSF}, as a child key, which is also explained in AKMA Solution 15. The key, K_{AKMA}, is derived and stored in Network B (more specifically in AAuF) on the network side. On the UE side, K_{AKMA}, is derived in eUICC and stored in AKMA framework, as explained in AKMA Solution 7. Application-specific session keys will be derived in AKMA framework from K_{AKMA}.

6) After the K_{AKMA} (B) is stored in AKMA framework, User wants to enable Profile A.

7) When the User gives the command for enabling Profile A, the Profile B becomes disabled immediately.

8) After the Profile B is disabled, the information related to Profile B is kept in AKMA framework.

9) After the Profile switch, eUICC requests from radio modem to drop the connection with Network B and trigger the connection with Network A. In case there is no cellular connection to Network B, e.g., if in step (3), the IP connection is established over WiFi when the device is on flight mode, the radio modem does not need to do anything.

10) Connection between the radio modem and Network A is established.

11) After the connection is established, AKA is initiated between Profile A and Network A via the radio modem. If Profile A is also participating in AKMA authentication with some other services, then Profile A can start AKMA authentication in this step. As long as the device of the Profile B has internet connection, via data connection of Profile A or WiFi, User can start using the service, as explained in AKMA Solution 13.

The sequence of events, explained above and in Fig. 7, occurs, e.g., when user wants to connect to an application for the first time or when the validity time of K_{AKMA} is expired. The sequence of events, explained below and in Fig. 8, occurs e.g. when UE has valid K_{AKMA} and wants to reconnect to the application server. Fig. 8 is explained below.

1) User wants to use the Service, namely APP1.

2) UE requests AKMA framework to connect to the Application Server of APP1 (AApF).

3) The AKMA framework derives a session key K_{AF} with identifier of AApF and some other parameters.

4) Then, with K_{AF}, AKMA framework generates a Temporary Identifier for Profile B (TID(B)).

5) AKMA framework sends request to AApF with the TID(B).

6) After AApF receives the request, it sends the request along with its identifier to AAuF.

7) With the TID(B) and identifier of AApF, AAuF recognizes the request is sent by Profile B. So, AAuF sends the K_{AF} of Profile B and the corresponding validity time to AApF.

8) AApF sends the Response back to UE. If the response is positive, then User can start using the service.

The UE and AApF can use the session key K_{AF} during the validity time. After the validity time expires or UE sends request by using another key, the AApF sends a request to AAuF for the recent key.

A profile in eUICC can be enabled, disabled, and deleted. In case of the solution offered above, each status of profile should have an effect on AKMA framework. The relation between profile status change and the action in AKMA framework is described below and summarized in Table I.

- When the profile is enabled, AKMA authentication starts immediately and the key, K_{AKMA}, for AKMA framework is renewed. Key in the network is also renewed.
- When the profile is disabled, AKMA framework keeps the key, K_{AKMA}. Network would not know that the profile is disabled, so network keeps the key.
- When the profile is deleted from eUICC, the AKMA framework also deletes the information related to that profile. Network would be aware that the profile is deleted from the eUICC. Therefore, network would know that key is not valid anymore.

TABLE I. RELATION BETWEEN PROFILE STATUS CHANGE AND THE ACTION IN AKMA FRAMEWORK

Profile Status	Action in AKMA Framework
Enabled	AKMA Authentication starts and the key, K_{AKMA}, in AKMA framework is renewed
Disabled	AKMA framework keeps the key, K_{AKMA}
Deleted	AKMA framework deletes all the information related to the profile.

The AKMA framework would keep K_{AKMA} and related temporary identifiers along with the K_{AF}. The AKMA framework may keep several keys for several profiles. For example, there can be Profile C that is also used for AKMA purposes. Any Profile, which is stored in eUICC, would be able to participate in AKMA. In this situation, AKMA framework should keep the keys of different Profiles apart and safe. AKMA framework would return AKMA registration information according to the request related to the Profile. If the Profile A is participating in the AKMA, request message, which is sent to AKMA framework, should include an indicator about Profile A. User should be able to choose which Profile to use for AKMA.

B. Multi SIM Case

In this section, we outline how our solution works for Multi SIM devices. As discussed earlier, there are different types of Multi SIM devices. Next, we will explain our solution for each type.

1) DSSS: DSSS can follow similar steps as suggested for eUICC in Section V.A.

2) DSDS: In the case of DSDS, AKMA authentication can be completed with less problems compared to the solution for eUICC. For DSDS, if one USIM, or primary USIM, is activated, registration of the other USIM is not lost [4]. Therefore, K_{AUSF} of secondary USIM from the bootstrapping is not lost every time primary USIM is activated. In this case, AKMA framework in AKMA Solution 7 is not a necessity for DSDS mode. Also, K_{AKMA} can be derived from K_{AUSF} freshly, any time AKMA authentication is needed, as explained in AKMA Solution 15. This solution can be applied for DSDS mode as well, because fresh key for each authentication is always preferred from security point of view, and less primary authentication is less workload for the network. With AKMA Solution 13, AKMA authentication can be done through an IP connection of the device, which can be either data connection of primary USIM or a WiFi connection.

3) DSDA: With DSDA, there is no need for special arrangement. AKMA authentication can be done as if the phone has single USIM. Since the both USIMs can be active simultaneously, bootstrapping can be initiated any time necessary. If USIM for AKMA does not have data connection, then AKMA authentication can be completed via IP connection of the device, as explained in AKMA Solution 13. For simplicity, requirements for DSDA can be adopted from DSDS.

VI. THREATS

One possible threat is from outside. In general, mobile device is more vulnerable than UICC. Therefore, the device could get compromised, while UICC is not. This way, hacker can get the keys and identifiers for a specific service and start using that service, masquerading as the victim. Another outsider threat might be in application side. A malicious application client could try to reach all the keys that exist in device. In addition, network might try to use UICC for reaching to the AKMA keys of other networks, which are stored in AKMA framework.

Another possible threat is from inside. The owner of the phone might prefer to store the keys separately, while changing UICCs. This way, the user can get access to the application without having UICC present.

Overall, those are valid threats that need to be mitigated. However, AKMA needs to be protected against those threats independently from our proposed solution.

Lifetime of the keys are determined by the service providers. In order to provide secure service, lifetime of the keys should be kept limited and refreshed regularly. However, this authority of the service provider can be spoiled by a malicious service provider.

The main threat that is specific to our solution is the following. In our solution, AKMA framework keeps K_{AKMA} after the Profile is disabled in eUICC. This means that the potential hacker could get hold of the K_{AKMA} key long after UE has intended to stop using it. This threat corresponds to a threat in the physical UICC case where a user removes the UICC from the device and gives the device to somebody else, e.g. sells the

device further. Now it is obviously a bad idea to leave derived keys in the device while the UICC has already been taken out.

Our solution provides mitigation against the threat by deleting K_{AKMA} from AKMA framework, when the corresponding Profile is deleted from eUICC. (See Section V.A.) It is the deletion of the Profile, rather than disabling that should happen when the device is given to hands of potentially untrustworthy party. There is a residual risk involved, e.g., in case where several people share the same device, and each have their own profile in the eUICC. In this case, it is natural to disable, rather than delete, the profile when control of the device is given to somebody else. However, it should be noted that in this type of setting the users of the same device typically have some level of trust between them.

The deletion of a Profile is an operation that involves the MNO [10]. Therefore, the MNO could also help in mitigating the threat by informing AApF about deletion of a Profile, so that AApF could delete the keys related to that Profile.

VII. Discussion about eUICC and Multi SIM

The proposals for standardizing Multi SIM are given to 3GPP [3], [6], and [7]. Even though proposals for RAN group are not accepted by 3GPP yet, but SA1 group has started working on Multi SIM and published technical report TR 22.834 recently [5]. The studies will be completed and Multi SIM standardization will be available.

In markets, DSDS UEs are available. These devices can support Voice over LTE (VoLTE) and Mobile Broadcast and Multicast (MBMS) services. Moreover, with the development of 5G, Radio Access Technologies (RAT) such as Narrow Band Internet of Things (NB-IoT) and 5G New Radio (NR) are introduced and improved. All these improvements will probably lead Multi SIM devices to be preferred more than single SIM devices in the future [17]. Some studies about Multi SIM and Dual SIM devices have been published [16], [17]. Furthermore, there are published analyses of eUICC [13], [20].

It is stated in the requirement with code EUICC4 [9] that Profiles in eUICC should behave like USIM in UICC. If eUICC is compared to Multi SIM cases, it can be seen that eUICC is behaving like DSSS. Currently, DSDS or DSDA devices are used commonly. Therefore, enhancements should be applied to specifications of eUICC, so that eUICC can adapt at least properties of DSDS or DSDA. It would be even better if eUICC specifications would also adapt to other Multi SIM scenarios than Dual SIM.

If eUICC cannot be adapted to DSDS or DSDA, it can still be combined with Multi SIM. For example, if the device has Dual SIM property, then it must have two UICCs. If one or both UICCs are turned into eUICC, then there can be many combinations for using different Profiles. This way, eUICC can mimic DSDS or DSDA. In case more than two UICCs are implemented in the device, eUICC could replace one of these, or even several eUICCs could be implemented in the same device.

According to the assessment of eUICC by Meyer et al. [13], eUICC is presumably the next generation SIM that can be used in all devices such as Internet of Things (IoT) and smart phones. Moreover, eUICC is currently included in many devices and is supported by various MNOs all over the world [21]. Therefore, eUICC should be taken into consideration by 3GPP along with Multi SIM concept and specifications should be developed accordingly.

VIII. Conclusion

In this paper, we deal with Authentication and Key Management for Applications (AKMA), which has been developed in 3GPP for single SIM devices. We consider the use cases of AKMA with Multi SIM devices and devices with eUICC. We paid attention to the scenario in which there are two Profiles in an eUICC (similarly two SIMs in Multi SIM devices) and one Profile is used for primary usage, such as voice and data, where the other Profile is used for AKMA services. Moreover, the scenario can be extended to a case with several Profiles/SIMs dedicated for AKMA. Regarding the specifications of eUICC and Multi SIM devices, it is not possible to use AKMA without interrupting other services, or vice versa.

In order to avoid this showstopper against the scenario, we propose a solution. We have used the 3GPP studies that are considered for AKMA for our solution. The solution is developed according to the current technical requirements of eUICC and Multi SIM devices. We expect that our solution will provide secure and uninterrupted services for Multi SIM devices and devices with eUICC.

Development of 5G technology is expected to introduce new or improved services, e.g. AKMA with eUICC and Multi SIM devices. However, combination and co-existence of some of these new services could be problematic. We have identified one such problematic combination, which, nevertheless, could be widely useful. Then we developed a solution to the problem and showed that it requires no changes in existing standards. The AKMA standards would be impacted by our solution but these are still work-in-progress.

Future work could include the implementation and standardization of our solution. In addition, new and better solutions could be developed for our problem, e.g. when eUICC specifications are developed further. Our solution could also be optimized further, especially in the case of Dual SIM Dual Standby. Another direction for further work is the setting where potentially several eUICCs and several physical UICCs co-exist in the same high-end device.

Appendix – Acronyms

3GPP: 3rd Generation Partnership Project
AApF: AKMA Application Function
AAuF: AKMA Authentication Function
AKA: Authentication and Key Agreement
AKAF: AKMA Anchor Function
AKMA: Authentication and Key Management for Applications
AUSF: Authentication Server Function
DSDA: Dual SIM Dual Active
DSDS: Dual SIM Dual Standby

DSSS: Dual SIM Single Standby
ETSI: European Telecommunications Standards Institute
eUICC: Embedded Universal Integrated Circuit Card
GBA: Generic Bootstrapping Architecture
GSMA: GSM Association
IoT: Internet of Things
LTE: Long Term Evolution; the 4th generation of cellular network's standards
ME: Mobile Equipment
MNO: Mobile Network Operator
RSP: Remote SIM Provisioning
SIM: Subscriber Identity Module
UE: User Equipment
UICC: Universal Integrated Circuit Card
USIM: Universal Subscriber Identity Module

REFERENCES

[1] GSM Arena website, "LG's first triple-SIM phone to be released next month", Web: https://www.gsmarena.com/lgs_first_triplesim_phone_to_be_released_next_month-news-3749.php. Accessed: Jul. 31, 2019.

[2] GSM Arena website, "OTECH F1 phone has Quad SIM support, probably glows in the dark, too", Web: http://blog.gsmarena.com/otech-f1-phone-phone-has-quad-sim-support-probably-glows-in-the-dark-too/. Accessed: Jul. 31, 2019.

[3] 3GPP TSG RAN Meeting 83 RP-190248, Working Group Meeting, Motivation for SI on multi-SIM devices in RAN, 2019.

[4] GSMA TS.37 Requirements for Multi SIM Devices, Version 5.0, 2018.

[5] 3GPP TR 22.834, Study on Support for Multi-USIM Devices, V17.0.0, 2019.

[6] 3GPP TSG-SA Meeting 84 SP-190309, Work Item Description, Propose WID on Support for Multi-USIM Devices, 2019.

[7] 3GPP TSG-SA WG1 Meeting 86 S1-191291, Working Group Meeting, MUSIM 22834 P-CR: Definitions, 2019.

[8] ETSI TS 103 383, Smart Cards; Embedded UICC; Requirements Specification, Version 14.0.0, 2018.

[9] GSMA SGP.21 RSP Architecture, Version 2.1, 2017.

[10] GSMA eSIM Whitepaper, The what and how of Remote SIM Provisioning, 2018.

[11] GSMA SGP.02 Remote Provisioning Architecture for Embedded UICC Technical Specification, Version 3.1, 2016.

[12] GSMA SGP.22 RSP Technical Specification, Version 2.2, 2017.

[13] M. Meyer, E.A. Quaglia, and B. Smyth, "An Overview of GSMA's M2M Remote provisioning specification", 2019, Web: https://arxiv.org/pdf/1906.02254.pdf.

[14] 3GPP TR 33.835, Study on authentication and key management for applications based on 3GPP in 5G, V0.4.0, 2019.

[15] H.L. Deepak, Hanumesh Rao, and B.A.Sujathakumari, "Dual SIM Dual Active Feture in a 3G Modem: Comprehensive Survey", *International Journal of Engineering Research and Modern Education*, 1 (2016), pp. 6-9.

[16] D. Göller, and K. Andersson, "Mobile telephony in emerging markets: The importance of dual-SIM phones", *in Beiträge zur Jahrestagung des Vereins für Socialpolitik 2018: Digitale Wirtschaft*, Feb. 2018.

[17] L. Pathak, T. Vrind, D. Sharma and D. Das, "Efficient Protocol for Performance Enhancement of B4G and 5G Networks for MultiSIM Deployment", *in 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, Feb. 2019, pp. 1-7.

[18] GSMA SGP.01, Embedded SIM Remote Provisioning Architecture, Version 4.0, 2019.

[19] 3GPP TS 33.220, Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA), V15.4.0, 2018.

[20] M. Meyer, E.A. Quaglia, and B. Smyth, "Attacks against GSMA's M2M Remote Provisioning", *in 22nd International Conference on Financial Cryptography and Data Security (FC'18)*, Feb. 2018, pp. 243-252.

[21] Roaming Buzz website, "What mobile devices that support eSIM?", Web: http://www.roamingbuzz.com/what-mobile-devices-that-support-esim-flexiroam/. Accessed: Oct. 11, 2019.

[22] 3GPP TS 31.102, Characteristics of the Universal Subscriber Identity Module (USIM) application, V15.5.0, 2019.