

# Secure Profile Provisioning Architecture for Embedded UICC

Jaemin Park, Kiyoung Baek, Cheoloh Kang  
System R&D Division  
The Attached Institute of ETRI  
Daejeon, Republic of Korea  
Email: {jmpark, cloud, cyberkan}@ensec.re.kr

**Abstract**—Embedded UICC (eUICC) is a new form of UICC, soldered into a device during manufacturing. On the contrary to the traditional UICC, the eUICC is not fully controlled by one specific MNO (Mobile Network Operator) since not removable physically from the device and not issued by the MNO. Thus, the profiles necessary for its operations should be provisioned remotely into the eUICC by new entity. For this remote provisioning, SM (Subscription Manager) is newly introduced by the standardization organization. However, this new ecosystem around eUICCs can cause tremendous security issues unless thorough consideration of security is accompanied during the standardization because the profiles usually include the security-sensitive information.

In this paper, a novel secure profile provisioning architecture for eUICCs is proposed. Our architecture mainly defines the overall architecture of the secure profile provisioning for eUICCs.

**Keywords**—Security, Provisioning, Embedded UICC, Subscription Manager, Secure Architecture

## I. INTRODUCTION

Embedded UICC (hereafter eUICC) [2] is a new form of UICC (Universal Integrated Circuit Card) [1], soldered into a device during manufacturing. The eUICC was initially considered to be utilized as the same roles of UICC for the M2M (Machine-to-Machine) device so as to endure the hostile environments such as high temperature, humidity, etc. or be adopted into the small device such as smart meter, etc. These days, the fields of its usages are being considered to be extended to the CEDs (Consumer Electronic Devices) for the smaller form factor to save the physical space of a device.

The traditional UICC is pre-provisioned by the SIM Vendor on the behalf of MNO by using the the MNO's data and applications (hereafter profiles) such as NAA(Network Access Application) [1] with related data (e.g. IMSI (International Mobile Subscriber Identity), keys, authentication algorithm, etc.) and fundamental VASs (Value-Added Services) [4]. That is, the UICC is tightly coupled with and fully controllable by one specific MNO. On the contrary to this, the eUICC is tightly coupled with its installed device rather than MNOs and not fully controlled by one specific MNO since not removable physically from the device. Thus any MNO or even other parties wish to and should be able to provision their profiles remotely into the eUICC. This remote profile provisioning is also essential for the eUICC to support the handset switching, national swapping and international swapping. The inherent feature of the eUICC and the absence of the control entity

for the eUICC inevitably leads to a new ecosystem, and the SM (Subscription Manager) is newly defined to manages and controls the profiles by the standardization [2], [3]. According to [2], SM is further divided into two roles, SM-DP (Data Preparation) for the profile generation and SM-SR (Secure Routing) for the profile transportation, and each role can be performed by separate physical or logical entities. Because the profile is security-sensitive to the SM-DP itself and the customer, it is obvious that each SM-DP is hardly willing to reveal their generated profile to others even SM-SR.

In this new ecosystem around eUICC, the tremendous security issues can be raised unless thorough consideration of security about the profile provisioning is accompanied during the standardization and the technical development. Since the profile includes the security-sensitive information, without protection during provisioning, the sensitive information can be revealed to malicious adversaries or competitors of business. Furthermore, a newly introduced SM essentially raises the security threats because of its right to control eUICCs and roles to provision the profiles. The profile provisioning should also consider the inherent non-removable feature and the diversity of capability of eUICC, otherwise there should be a repository to manage the huge amount of information related to the profile provisioning.

Motivated by above security concerns, we propose a novel secure provisioning architecture to guarantee the security of the profile provisioning regardless of the capabilities of eUICCs. The rest of this paper is organized as follows: In Section II, we present the preliminaries about the eUICC provisioning ecosystem, the standardization status and the related works. In Section III, the problem statement is described. In Section IV, we propose our profile provisioning architecture and internal architecture of eUICC. In Section V, the analysis of our proposed architecture is given. Finally, the conclusions and further works are given in Section VI.

## II. PRELIMINARIES

### A. eUICC Provisioning Ecosystem

The eUICC provisioning ecosystem mainly consists of eUICCs, eUICC Vendors, Devices and SMs (SM-SRs and SM-DPs) [2], [4] as shown in Fig. 1. SM is divided into two parties; one is SM-SR for secure routing and the other is SM-DP, the owner or generator of security-sensitive information, for data preparation. As shown in Fig. 1, small numbers of SM-SRs are interworking with each other and SM-DPs delegate the roles

of secure routing of the sensitive information to their trusted SM-SRs. For the provisioning and management, one eUICC usually interworks with one SM-SR. Because of their specific roles, one SM-SR can interwork with several SM-DPs for secure routing of profiles generated by SM-DPs to eUICCs. For scalability, several SM-SRs can interwork each other to extend the manageability to other eUICCs associated with other SM-SRs. For secure routing, SM-SRs usually utilize the SM-SR Credentials, installed in eUICCs during the manufacturing and shared by eUICC Vendors.

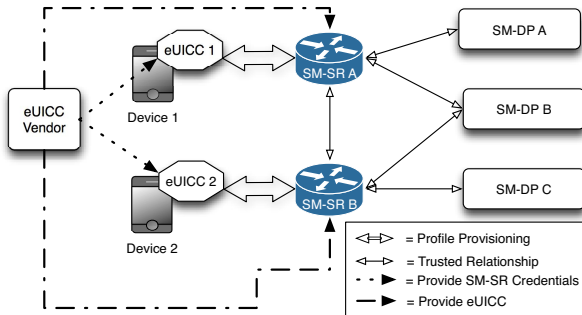


Fig. 1. eUICC Profile Ecosystem

### B. Standardization and Related Works

The eUICC is standardized by the ETSI (European Telecommunications Standards Institute) SCP (Smart Card Platform), and the working document is ETSI TS 103.383 V12.0.0 [2]. This standard defines the use cases and requirements about the eUICC and interworking with SMs. GSMA (Groupe Spéciale Mobile Association) publishes the document about requirements for eUICC, which defines a number of requirements and use cases for developing eUICC systems [3]. These standards only define the conceptual models, use cases and requirements. Since only conceptual architecture of eUICC is available, there exist few works about eUICC. According to [4], several patents and proofs of concept have been released, but those are not related to the security or published in public to be reviewed or analyzed.

As mentioned above, the current status of standardization is still immature. Thus, any detail and published secure profile provisioning directly related to eUICC cannot be found, but only few works which describes the enhanced business process for a flexible MCIM (M2M Communication Identity Module) [7] and several works related to the provisioning for UICCs or smart cards can be found [6], [8]–[13]. In [7], the business process related to M2M is mainly focused, therefore no detail consideration of security can be found. In [6], the methodology to utilize current UICC technology to provision UICC-based applications after issuing of UICCs is proposed where GP Secure Channel Protocol (hereafter SCP) is applied to the payment applications for post-distribution provisioning and personalization with the utilization of public key-based key agreement between Bank and UICC. In [8], [9], the On-board Credentials (ObCs) are proposed to utilize the general-purpose secure hardware as credentials by provisioning the credentials into ObC devices. In [10]–[13], new paradigm of smart card ownership where the ownership is delegated

to users not card issuers and its related security protocols are proposed. However, these approaches are difficult to be directly applied to the eUICC provisioning ecosystems even though some portions of works can be utilized to design other architectures or detail protocols. The reasons mainly include; no consideration of fundamental eUICC ecosystem, essential key separation among SM-SRs and SM-DPs, various kinds of capabilities which eUICCs possess, and protection of that capability information. Therefore, we consider the way to apply the de-facto standard for profile provisioning, GP SCP [5] to the eUICC provisioning ecosystem for comparison.

### C. Method to Apply GP SCP to eUICC

Before describing the methodology, we first need to explain SD (Security Domain) and SCP briefly. SD is an application running inside the UICC to act as the on-card representatives of off-card entities. SD mainly supports security services such as key handling, encryption, decryption, digital signature, etc. and can be divided into two categories; ISD (Issuer SD) is the primary, mandatory on-card representative of the Card Issuer (e.g. MNO) and SSDs (Supplementary SDs) are additional, optional on-card representatives of Application Providers (e.g. Bank). SCP provides the secure communication channel between these SDs and off-card entities to manage UICCs and their applications securely. SCP usually provides the confidentiality, entity authentication, data origin authentication and integrity. By sending and receiving the APDU (Application Protocol Data Unit) commands between SD and off-card entity via SCP, the content can be loaded and installed into the UICC.

To apply the GP SCP for eUICC, we need to define the relationship between SDs and components of eUICC provisioning ecosystem; ISD is the on-card representative of SM-SR and SSD is of SM-DP. To utilize SCP connections, the ISD key between eUICC and SM-SR should be inserted into the eUICC during manufacturing processes or other secure manners. The SSD key should be shared between SM-SR and SM-DP in advance of profile provisioning using additional secure manners or other key agreement protocol between SSD and SM-DP should be utilized mentioned in [6].

Using above circumstances, the method to apply the GP SCP can be depicted as shown in Fig. 2. The eUICC establishes the network access to SM-SR. SM-SR establishes the 1st SCP session with ISD of eUICC using ISD key. SM-SR installs new SSD with one of the privileges like Authorization Management or Delegated Management into eUICC by communicating with ISD of eUICC since only the SSDs of the listed privileges can load and install the profile into the eUICC. After this, SM-SR also inserts the SSD key of SM-DP into the installed SSD for SM-DP if the key agreement protocol mentioned in [6] is not utilized. The 1st SCP session is completed and terminated. Now, the eUICC establishes the additional network access to SM-DP. SM-DP establishes a new SCP session with the SSD using the SSD key. SM-DP sends the blocks of profile and APDU commands to the SSD via the 2nd SCP session. If the SSD has the privilege of Delegated Management, SM-SR should send a Token to SM-DP for the authorization. After successful completion of profile provisioning, the 2nd SCP session would be terminated.

Even though this approach can work properly, applying the GP SCP directly into eUICC provisioning ecosystem

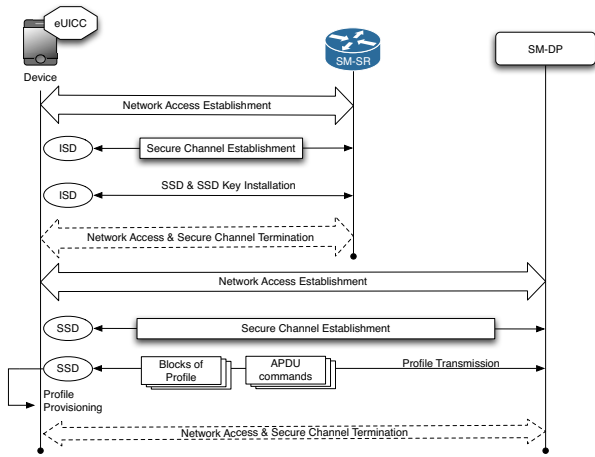


Fig. 2. GP SCP for eUICC Profile Provisioning

has several drawbacks with respect to scalability, efficiency, security and flexibility as follows:

**Scalability** - To share the SSD key, SM-SR and SM-DP should implement additional secure channel each other. These additional and inconvenient efforts can hinder the scalability.

**Efficiency** - Two communication channels and two SCP sessions should be guaranteed. That is, SM-DP also needs to implement the communication infrastructure to interwork with eUICCs. Additional communication channel and SCP connection can be the burden of eUICCs and SMs.

**Security** - Since the initial SSD key is shared between SM-SR and SM-DP, the blocks of profile transferred by SCP can be revealed to other entities if installing new SSD key into eUICC by SM-DP is not performed before profile provisioning.

**Flexibility** - Only specific cryptographic algorithms defined in GP specification can be utilized for profile provisioning. This limitation can be dangerous if security threats of the algorithms are found. Furthermore, the variation due to the local regulation about the cryptographic algorithms is impossible.

### III. PROBLEM STATEMENT

In this section, we define the requirements of the profile provisioning architecture for eUICC.

#### A. General Requirement

As mentioned above, profile provisioning architecture for eUICC should be proposed with the consideration of new provisioning ecosystem. Furthermore, only minimum processing overhead for the security-related operations should be a burden to the eUICC during the profile provisioning since the eUICC is also the resource-constraint medium. Finally, to address the drawbacks of the existing technology, the scalability, the efficiency, and the flexibility in Section II should be enhanced.

#### B. Security Requirement

Because the profile mostly includes the security-sensitive information, the protection should be supported. Therefore,

the following security requirements can be guaranteed: The following security requirements should be guaranteed in accordance with the requirements in [5]:

**Mutual Authentication** - eUICC and SM-DP prove their authenticities each other through cryptographic exchanges.

**Confidentiality** - profiles being transmitted to eUICC by SM-DP are only available to those authorized entities.

**Data Integrity** - data being exchanged between eUICC and SM-DP has not been altered by unauthorized entities.

**Data Origin Authentication** - eUICC and SM-DP ensure that data actually came from the authorized entities, SM-DP and eUICC, respectively.

**Non-Exposure of Key** - credentials between eUICC and SM-DP are expose only to directly involved entities in the profile provisioning; eUICC and SM-DP.

**Verification of eUICC's Information** - information of eUICC sent to other entities is able to be verified by the receivers.

### IV. PROPOSED PROFILE PROVISIONING ARCHITECTURE

In this section, we propose our architecture, Secure Profile Provisioning Architecture for eUICC (hereafter SPA) to address the issues raised in Section III and meet the security requirements listed below. SPA mainly defines the overall architecture for the secure profile provisioning. Therefore, the changeable security protocols like secure communication protocol and key agreement protocol are out of scope.

#### A. Terminologies

We define the terminologies in Table I. Some terminologies are come from [2] and reproduced here for simplicity.

TABLE I. TERMINOLOGIES

Terminology	Description
eUICC ID	Identification for eUICC to identify a particular eUICC
(eUICC Certification Center	The trusted third party to evaluate eUICCs (e.g. GSMAS SAS (Security Accreditation Scheme))
Provisioning Profile	The profile to be utilized to access SMs for the profile provisioning via mobile networks
SM-SR Credential	The credential to establish the secure communication channel between eUICC and SM-SR
SM-DP Credential	The credential to protect the profile generated by SM-DP
Capability Information	The information stored in the eUICC, including supporting cryptographic algorithms, key agreement protocols, the capacity information, etc.
Key Agreement Module (KAM)	The software running in the eUICC to perform the key agreement protocol to agree SM-DP Credentials with SM-DP
Device Module (DM)	The software running in the Device to perform the roles of the intermediary between eUICC and SM-SR
Profile Installer (PI)	The software running in the eUICC to perform the decryption and verification of the protected profile blocks from SM-DP and provision the profile blocks
Profile Manager (PM)	The software running in the eUICC to manage profiles as blocks of encrypted data and has relationship with SM-SR

#### B. Secure Profile Provisioning Architecture (SPA)

SPA mainly consists of two procedures; Pre-Provisioning Procedure and Secure Profile Provisioning Procedure.

1) *Pre-Provisioning Procedure*: SPA involves the pre-provisioning procedure, conducted during the eUICC-based device manufacturing. Through this procedure, SM can collect the necessary information for SPA, and the verification of the capability information of the eUICC can be possible when performing the secure profile provisioning in the field. The detail of this pre-provisioning procedure is depicted in Fig. 3.

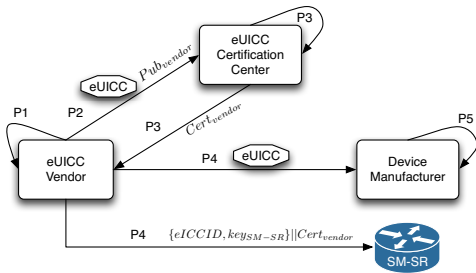


Fig. 3. Pre-Provisioning Procedure

*Step P1* - The eUICC Vendor develops eUICCs. During this, the SM-SR Credentials ( $key_{SM-SR}$ ) and the capability information ( $CI_{installed}$ ) of each eUICC are installed into each eUICC. Then, the eUICC Vendor generates the public key pair, and installs the private key ( $Priv_{vendor}$ ) into the eUICCs.

*Step P2* - The eUICC Vendor requests the evaluation of the eUICCs to the eUICC Certification Center with the public key ( $Pub_{vendor}$ ) of Step P1.

*Step P3* - Only after the successful evaluation, the eUICC Certification Center responds the results with the certificate ( $Cert_{vendor}$ ) by using  $Pub_{vendor}$ .

*Step P4* - The eUICC Vendor can install the received certificate into the eUICCs, and sends the developed and evaluated eUICCs to the device manufacturers. Simultaneously, the eUICC Vendor sends the information to SM-SR required for SPA such as the certificate, the eUICC IDs, the SM-SR Credentials, the mapping table between eUICC IDs and SM-SR Credential indexes, etc. in the secure manner.

*Step P5* - The Device Manufacturer develops the eUICC-based devices using the received eUICCs.

2) *Secure Profile Provisioning Procedure*: After the pre-provisioning procedure, the eUICC-installed devices are deployed in the field. For their operations, the profiles should be provisioned to the eUICCs. Fig. 4 depicts the secure profile provisioning procedure in detail. For the simplicity, we only denote one eUICC and one SM (one SM-SR and one SM-DP); however, the number of the entities can be extended depending on the needs of the market.

*Step 1* - The eUICC initially accesses SM-SR using the Provisioning Profile. In addition, the eUICC can access SM-SR via WiFi, USB, etc. without the Provisioning Profile. Also, the provisioned profile for accessing the mobile network can be utilized to reach to SM-SR.

*Step 2* - After the establishment of the communication channel, the eUICC sends the message including the eUICC ID ( $eUICCID$ ) and its capability information ( $CI_{proposal}$ ) to SM-SR for the capability negotiation. The eUICC ID and capability

information are signed by the eUICC Vendors private key, and this signed value needs to be added to the message. If there is no KAM installed onto the eUICC, the eUICC can replace the key agreement protocol of the  $CI$  message with proper value such as null, blank, error message, etc. to inform SM that the installation is required. Simultaneously, the eUICC can also send the eUICC Vendors certificate if necessary.

*Step 3* - SM acquires the eUICC Vendors certificate from the eUICC Certification Center or the message sent by the eUICC in Step 2. With that certificate, SM-DP verifies the signature of the eUICC ID and the capability information.

*Step 4* - Then, SM-DP sends the message including the selected capabilities ( $CI_{selected}$ , the cryptographic algorithms, the key agreement protocol, the secure communication protocol and so forth) and its hashed value to the eUICC via SM-SR if the decision is completed based on the received capability information. The capability information about the secure communication protocol can be chosen through the interworking between SM-SR and SM-DP.

*Step 5* - PM of eUICC and the SM-SR establish the secure communication channel based on the selected protocol. The SM-SR Credential can be same as or derived from the master secret installed in Step P1.

*Step 5* - The blocks of KAM from SM-DP and the acknowledgement from the eUICC can be sent through the secure communication channel established in Step 5 and installed to the eUICC if the message of Step 2 indicates that the installation is necessary. This can be happened when the change of security policy is required, the vulnerabilities of the cryptographic algorithm used in that module are found, or other reasons are happened.

*Step 6* - KAM of eUICC and SM-DP perform the key agreement protocol dynamically to generate the SM-DP Credentials ( $key_{SM-DP}$ ) through the established secure communication channel between the eUICC and SM-SR.

*Step 7* - Using the agreed SM-DP Credentials and the selected cryptographic algorithms, SM-DP encrypts each block of profile ( $Profile_i$ ) and generates its MACed value. Then, SM-DP sends the protected profile blocks to the eUICC via the secure communication channel of SM-SR. PM of eUICC performs the necessary cryptographic operations for the secure communication channel, and then PI of eUICC decrypts and verifies the received profile blocks. If no problem found, the profile blocks are provisioned inside the eUICC by PI. Then, PI sends the acknowledge for each block of profile with its MACed value to SM-DP. This step continues recursively until the provisioning is completed.

### C. Proposed Internal Architecture of eUICC

The change of the internal architecture of the eUICC compared to the conceptual architecture in [2] is inevitable to support SPA as depicted in Fig. 5. Since new module, KAM is added to the internal architecture of eUICC, interworking among modules should be considered to reflect this change. DM of the device should be implemented to handle the messages from SM-SR. Handled messages are sent to PI for provisioning, and PI interworks with KAM to retrieve the agreed SM-DP Credentials for decrypting and verifying the

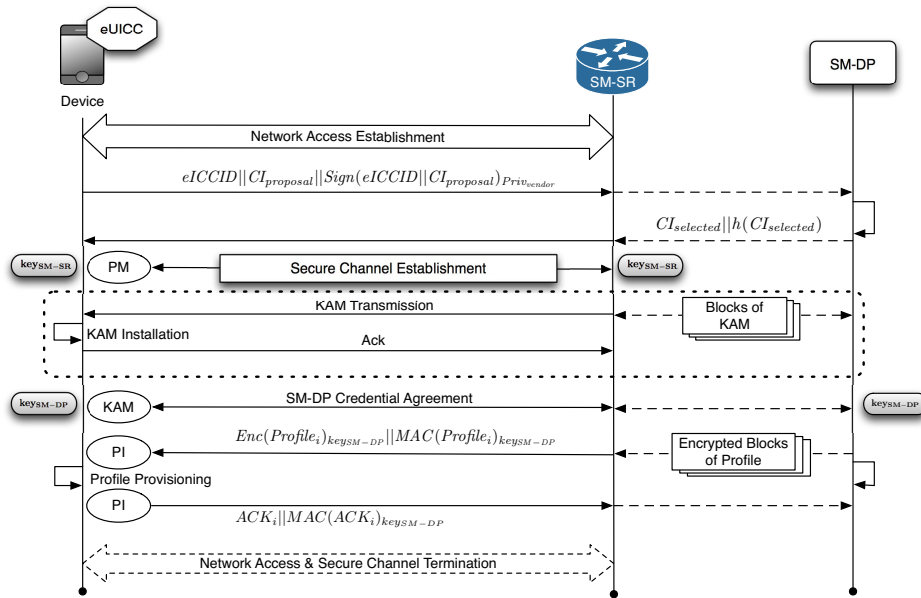


Fig. 4. Secure Profile Provisioning Procedure

protected profile blocks. After completing of cryptographic operations, PI provisions the profile into the eUICC.

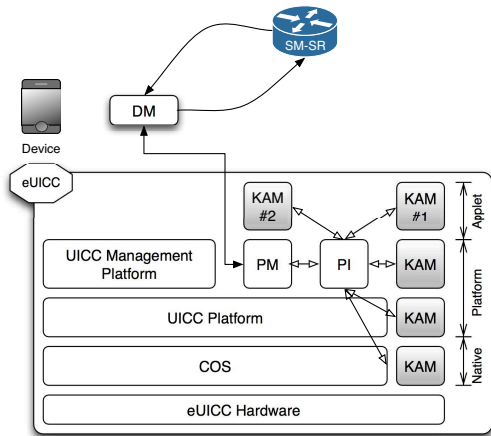


Fig. 5. Internal Architecture of eUICC

1) *Key Agreement Module (KAM)*: KAM is software running inside the eUICC to perform the key agreement protocol, which is already known by eUICC and SM-DP after the capability negotiation of SPA, with SM-DP. KAM is mainly utilized to agree the SM-DP Credentials on demand. For the security, the SM-DP Credentials should not be revealed to any party, even SM-SR, except for eUICC. To accomplish this, KAM is designed and applied to SPA. KAM can provide the asymmetric algorithm-based key agreement protocol, or possess the master secrets of SM-DP Credentials, which are accessible only after the authentication and where SM-DP Credentials are derived afterward.

KAM can be different from each SM-DP if the capabilities of the eUICC are affordable. That is, depending on the security policies, the security threats found in some specific algorithms, and other reasons, different KAMs can be installed. Depending on the selected cryptographic algorithms for protecting profiles, KAM should be able to agree all kinds of SM-DP Credentials. KAM can be various forms like installable applet, native program of COS (Chip OS) or component of the UICC platform (e.g. Javacard Platform or GP) as shown in Fig. 5.

2) *Capability Information*: Depending on the hardware specification and the implementations, the eUICC can be different from each other with respect to supporting cryptographic algorithms, affordable key agreement protocols, affordable secure communication protocols, total and available memory capacities, existences of KAM or related information, etc. If SM should manage all of this information, necessary storage can be drastic. Then, this complexity yields the increment of error and management cost. Therefore, this capability information should be stored inside the eUICC and be retrieved by the external entities if necessary. Without the guarantee of the correctness and the verification about this information, SM has no method to convince that the capability of the eUICC is correctly implemented. Therefore, the technical method to verify the capability information sent from the eUICC should be existed. To address these issues, we propose a methodology to store the capability information of each eUICC inside itself and verify this information if necessary.

## V. ANALYSIS

In this section, we evaluate our SPA against the requirements defined in Section III. Furthermore, we compare our SPA with the approach mentioned in Section II.

### A. Security Features

SPA provides the secure profile provisioning together with supporting the non-exposure of key and the verification of eUICC's information (capability information).

*Mutual Authentication* - Depending on the key agreement protocol supported by KAM, the mutual authentication between eUICC and SM-DP can be provided or not. However, there might exist no key agreement protocol without mutual authentication.

*Confidentiality* - Confidentiality is guaranteed since the profile being transmitted is encrypted by the SM-DP credential.

*Data Integrity* - Integrity is guaranteed by performing MAC operation for all blocks of profile by SM-DP and all acknowledgements by the eUICC. Therefore, eUICC and SM-DP ensure that data being received has not been altered.

*Data Origin Authentication* - Data origin authentication is guaranteed by performing MAC operation using the agreed SM-DP Credential for all blocks of profile by SM-DP and all acknowledgements by the eUICC. Therefore, eUICC and SM-DP ensure that all data actually came from SM-DP and eUICC, respectively.

*Non-Exposure of Key* - Because KAM embeds the shared secret onto the eUICC or performs the key agreement protocol with SM-DP, any SM-DP Credential cannot be shared with other entities.

*Verification of Capability Information* - Since the capability information of eUICC is signed by eUICC Vendors private key stored inside the eUICC, SMs can ensure that the received capability information was evaluated successfully by eUICC Certification Center and has not been altered.

### B. Cryptographic Performance of eUICC

To support SPA, the overhead of the eUICC can be increased since the eUICC should perform additional cryptographic operations. The cryptographic performance can be evaluated by measuring the time required for the eUICC to perform necessary cryptographic operations. Therefore, the overall cryptographic performance is calculated as follows:

$$P(A) = \sum t(f) \quad (1)$$

where  $P(A)$  is the overall time for the eUICC to perform  $A$  and  $t(f)$  is the measured time for the eUICC to perform specific cryptographic operation,  $f$ .

Using (1),  $P(SPA)$  can be calculated as follows:

$$P(SPA) = P(SCP) + P(KAP) + N\{t(Dec) + t(MAC)\} + t(Sign) + t(h) \quad (2)$$

where  $N$  is number of blocks of profile,  $SCP$  is Secure Communication Protocol and  $KAP$  is Key Agreement Protocol.

If the cryptography algorithm for profile decryption is the symmetric and identical to GP SCP,  $P(SCP)$  can be approximated to (3) since secure communication protocols mostly include key agreement and protection of blocks of data with verification of MAC values.

$$P(SCP) \approx P(KAP) + N\{t(Dec_{sym}) + t(MAC)\} \quad (3)$$

Then, (2) can be simplified as follows:

$$P(SPA) \approx 2P(SCP) + t(Sign) + t(h) \quad (4)$$

For better understanding, we compare it with the performance of GP SCP ( $t$ ) in Section II. The cryptographic performance of GP SCP to be performed by eUICC can be as follows:

$$P(GP) = t = 2P(SCP) \quad (5)$$

By subtracting (5) from (4), we can evaluate the performance increment due to SPA in the case when the symmetric algorithm is utilized for the profile protection. Then, we can conclude that the cryptographic overhead increased by SPA can be as follows:

$$\sigma_{sym} \approx t(Sign) + t(h) \quad (6)$$

where  $\sigma_{sym}$  is the performance difference of the eUICC when the symmetric algorithm is applied.

Suppose that the asymmetric algorithm is utilized for protecting the blocks of profile. Even though not suitable for the large block of profile, the performance review against every possible candidates can be meaningful for new ecosystem. To estimate the overhead of the asymmetric case, we subtract (5) from (2) directly and assign (3), then we acquire following (7):

$$\sigma_{asym} \approx M\{t(Dec_{asym}) + t(MAC)\} - N\{t(Dec_{sym}) + t(MAC)\} + t(Sign) + t(h) \quad (7)$$

where  $\sigma_{asym}$  is the performance difference of the eUICC when the asymmetric algorithm is applied,  $M$  is the number of blocks of profile (length= $L$ ) for the asymmetric algorithm (block length= $b1$ ) and  $N$  is the number of blocks of same profile for the symmetric algorithm (block length= $b2$ ).

Since the block lengths of the symmetric and the asymmetric are different each other, and ciphering and MACing are processed for each block of profile, (7) can be expressed as follows using (6):

$$\sigma_{asym} \approx \sigma_{sym} + \left\lceil \frac{L}{b1} \right\rceil \cdot t(Dec_{asym}) - \left\lceil \frac{L}{b2} \right\rceil \cdot t(Dec_{sym}) + \left\{ \left\lceil \frac{L}{b1} \right\rceil - \left\lceil \frac{L}{b2} \right\rceil \right\} \cdot t(MAC) \quad (8)$$

where  $\lceil x \rceil$  is the ceiling function of  $x$ .

For the reference, according to the cryptographic performance of the CCP (Crypto Co-Processor) used for (e)UICC [14], we calculate the approximate value of each  $\sigma$  against the profile length,  $L$ , as shown in Fig. 6. We consider two cases to estimate  $\sigma_{asym}$  depending on the type of MAC algorithm; CMAC (Cipher-based MAC) or HMAC (Hash-based MAC). As the profile length,  $L$ , is increased, all  $\sigma_{asym}$  values are increased linearly. Therefore, for the better performance, the symmetric algorithm for encrypting and decrypting the profile is preferable since the constant overhead ( $\sigma_{sym}$ ) is promised.

### C. Comparison

We compare SPA with the approach of the GP SCP with respect to the security, the performance and the drawbacks mentioned in II. Besides the improved security, SPA overcomes

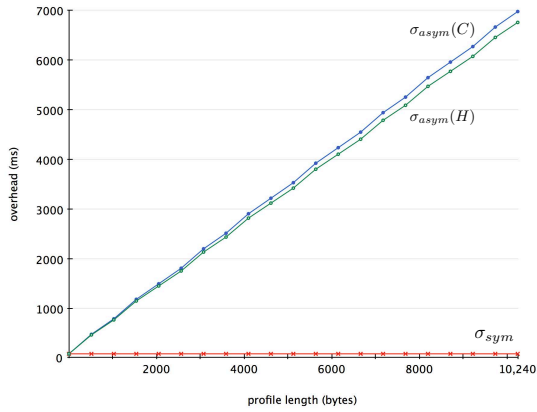


Fig. 6. Cryptography Performance of eUICC

all drawbacks of GP SCP with reasonable overhead,  $\sigma$  of the performance as shown in Table II.

SPA does not necessitate the pre-shared secret between SM-SR and SM-DP since SM-DP Credential is generated on demand. As this inconvenient procedure is removed, the scalability is improved. SM-DPs do not have to implement the communication facilities to be accessed by eUICCs directly since one communication channel and one SCP session with SM-SR are required. This can reduce the management cost of eUICC systems and the network overhead of eUICCs. By utilizing KAM and the capability information of eUICC, SPA supports various kinds of security protocols if eUICC is affordable. Therefore, diverse key agreement protocols, secure communication protocols and cryptographic algorithms can be applied depending on the circumstances around the eUICC.

TABLE II. COMPARISON

Criteria		GP SCP	SPA
Security	Mutual Authentication	O	O
	Confidentiality	O	O
	Data Integrity	O	O
	Data Origin Authentication	O	O
	Non-Exposure of Key	$\Delta$	O
	Verification of Capability Information	$\times$	O
Performance	Communication Channel	2	1
	Secure Communication Channel	2	1
	Cryptographic Overhead of (e)UICC	$t$	$t + \sigma$
General	Scalability	$\Delta$	O
	Efficiency	$\Delta$	O
	Flexibility	$\Delta$	O

## VI. CONCLUSION AND FURTHER WORKS

In this paper, we propose a novel secure profile provisioning architecture, SPA for the eUICC. For the profile provisioning, we primarily defines the overall architecture of the secure profile provisioning for eUICC. To protect the profile and overcome the drawbacks of current UICC technology, we utilize the capability negotiation using the capability information of eUICC and the special module, KAM, to agree SM-DP Credentials dynamically during the profile provisioning procedures. To show the excellence of SPA, we analyze our

SPA against security, cryptographic performance of eUICC, scalability, efficiency and flexibility. Our analysis depicts that SPA is superior to the methodology to apply GP SCP with reasonable overheads of eUICC if the symmetric algorithm for protecting profile is applied.

As further works, we intend to study about new secure communication protocol and key agreement protocol optimized for eUICC systems. This study should mainly deal with new circumstances raised by the eUICC provisioning ecosystem such as the inevitable remote management of numerous eUICCs, the security concerns for all related entities around, etc.

## ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions to improve the quality of the paper.

## REFERENCES

- [1] ETSI TR 102 216 V3.0.0, *Smart cards; Vocabulary for Smart Card Platform specifications*, ETSI, 2003.
- [2] ETSI TS 103 383 V12.0.0, *Smart Cards; Embedded UICC; Requirements Specification*, ETSI, 2013.
- [3] GSMA V1.0, *Embedded SIM Task Force: Requirements & Use Cases*, GSMA, 2011.
- [4] CSMG, *Reprogrammable SIMs: Technology, Evolution and Implications*, tech. report, CSMG, TMNG Global, 2012.
- [5] *GlobalPlatform, Card Specification Version 2.2.1*, GlobalPlatform, Jan. 2011.
- [6] V. Alimi and M. Pasquet, "Post-Distribution Provisioning and Personalization of a Payment Applications on a UICC-based Secure Element," *Int'l Conf. Availability, Reliability and Security, 2009 (ARES'09)*, IEEE, 2009, pp.701-705.
- [7] H. Bender and G. Lehmann, "Evolution of SIM provisioning towards a flexible MCIM provisioning in M2M vertical industries," *Int'l Conf. Intelligence in Next Generation Networks, 2012 (ICIN2012)*, IEEE, 2012, pp.57-64.
- [8] J.-E. Ekberg, N. Asokan, K. Kostianen and A. Rantala, *On-board Credentials with Open Provisioning*, tech. report, NRC-TR-2008-007, Research Center, NOKIA, 2008.
- [9] N. Asokan and J.-E. Ekberg, "A Platform for OnBoard Credentials," *Financial Cryptography and Data Security, 2008*, Springer-Verlag, 2008, pp.318-320.
- [10] R. N. Akram, K. Markantonakis and K. Mayers, "Application Management Framework in User Centric Smart Card Ownership Model," *Information Security Applications, 2009*, Springer-Verlag, 2009, pp.20-35.
- [11] R. N. Akram, K. Markantonakis and K. Mayers, "A Paradigm Shift in the Smart Card Ownership Model," *Int'l Conf. Computational Science and Its Applications, 2010 (ICCSA'10)*, IEEE, 2010, pp.191-200.
- [12] R. N. Akram, K. Markantonakis and K. Mayers, "Simulator Problem in User Centric Smart Card Ownership Model," *Int'l Conf. Embedded and Ubiquitous Computing, 2010 (EUC'10)*, IEEE, 2010, pp.679-686.
- [13] R. N. Akram, K. Markantonakis and K. Mayers, "A Privacy Preserving Application Acquisition Protocol," *Int'l Conf. Trust, Security and Privacy in Computing and Communications, 2012 (TrustCom'12)*, IEEE, 2012, pp.383-392.
- [14] STMicroelectronics, "Smartcard 32-Bit RISC MCU with 32, 64, 96, 128 Kbytes EEPROM, Javacard HW Execution & Cryptographic Library," ST22L128 datasheet, 2004.
- [15] C. Paar and J. Pelzl, *Understanding Cryptography*, 1st Edition, Springer, Jul. 2010 (2nd Printing edition).
- [16] B.Kaliski, PKCS#1: RSA Encryption Version 1.5, RFC2313, Network Working Group, 1998.