TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Ken-Tristan Peterson 179933IVSB

M2M embedded subscriber identity module provisioning in networks without SMS service

Bachelor's Thesis

Supervisors: Marika Kulmar, MSc
Tanel Peep, MSc

Tallinn 2020

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Ken-Tristan Peterson 179933IVSB

M2M SISSE EHITATUD ABONENDI IDENTIFITSEERIMISE MOODULI PROVISIONEERIMINE VÕRKUDES, KUS PUUDUB SMS TEENUS

Bakalaureusetöö

Juhendaja: Marika Kulmar, MSc
Tanel Peep, MSc

Tallinn 2020

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Ken-Tristan Peterson

13.05.2020

Abstract

The main goal of this thesis is to analyze possible solutions for provisioning the M2M embedded subscriber identity module in networks without SMS support.

The paper gives an overview of the current eSIM provisioning solution and communication initialization procedure. eSIM implementation difficulties, which are caused by relying on SMS or using new radio access technologies like NB-IoT, are analyzed. The research analyzes the SMS service security concerns and SIM attacks, which SMS is an enabler for.

Device and eSIM communication is traced with special hardware to present the current provisioning process and identify the parameters which are passed within a push SMS. Based on the practical tracing and statement of the problem, new provisioning solutions are proposed. In the end, these identified solutions are compared.

Throughout the research, security aspects are analyzed and taken into account in comparison of proposed solutions.

This thesis is written in English and is 31 pages long, including 6 chapters, 10 figures and 1 table.

Annotatsioon

M2M sisse ehitatud abonendi identifitseerimise mooduli provisioneerimine võrkudes, kus puudub SMS teenus

Lõputöö peamine eesmärk on analüüsida võimalikke lahendusi M2M sisse ehitatud abonendi identifitseerimise mooduli provisioneerimist sidevõrkudes, kus puudub SMS teenus.

Antud töö annab ülevaate hetkesest eSIM provisioneerimise lahendusest ning kommunikatsioonist. Analüüsitakse implementatsiooni takistusi, mis on tingitud SMS teenuse puudumisest IoT rändluslepingutes ja uutes sidevõrkudes nagu NB-IoT. Töö analüüsib SMS teenuse haavatavust ning SIM kaardi rünnakuid, mille võimaldajaks on SMS teenus.

Seadme ja eSIMi vahelist kommunikatsiooni jälgitakse spetsiaalse riistvaraga ja tulemusi presenteeritakse. Kommunikatsiooni jälgimise tulemustest ja probleemi püstitusest lähtuvalt, pakub autor välja uued provisioneerimis meetodid ning antud uusi lahendusi võrreldakse.

Töö käigus hinnatakse ja analüüsitakse küberturbe aspekte ja neid arvestatakse uute lahenduste valikul.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 31 leheküljel, 6 peatükki, 10 joonist, 1 tabel.

List of abbreviations and terms

2G	Second generation of cellular communications
3G	Third generation of cellular communications
4G	Fourth generation of cellular communications
5G	Fifth generation of cellular communications
AES	Advanced Encryption Standard
APDU	Application Protocol Data Unit
ATR	Answer To Reset
BIP	Bearer Independent Protocol
CBC	Cipher Block Chaining
CMAC	Cipher-based Message Authentication Code
EID	eUICC identifier
eSIM	Embedded Subscriber Identity Module
eUICC	Embedded Universal Integrated Circuit Card
EUM	eUICC Manufacturer
GSMA	GSM Association
ICCID	Integrated Circuit Card ID
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
ISD-R	Issuer Security Domain – Root
iSIM	Integrated Subscriber Identity Module
Ki	Authentication Key
KIc	Key and algorithm Identifier for ciphering
KID	Key and algorithm Identifier for Redundancy Check, Cryptographic Checksum and Digital Signature
LDS	Local Discovery Service
LPD	Local Profile Download
LPWAN	Low Power Wide Area Networks
LTE-M	LTE Cat-M1 technology

LUI	Local User Interface
M2M	Machine to Machine
MCC	Mobile Country Code
MNC	Mobile Network Code
MNO	Mobile Network Operator
MSIN	Mobile Subscriber Identification Number
MSISDN	Mobile Station International Subscriber Directory Number
NB-IoT	LTE Cat-NB1 technology
nuSIM	Different type of iSIM aimed at LPWAN technologies
OTA	Over The Air
PSK	Pre-Shared Key
RSP	Remote SIM Provisioning
SIM	Subscriber Identity Module
SMS	Short Message Service
SPI	Secure Parameter Index/Indicator
TLS	Transport Layer Security
UICC	Universal Integrated Circuit Card
URI	Uniform Resource Identifier
USIM	UMTS(3G) Subscriber Identity Module

Table of Contents

List of figures

List of tables

1 Introduction

The rise of Internet of Things and Machine to Machine economy has brought millions of devices that need to be connected to Radio Access Technologies like 2G, 3G, 4G or also new solutions like 5G, NB-IoT and LTE-M. These devices use subscriber identity modules, known as SIM cards, for registering in cellular networks.

While consumers have used SIM cards for decades without significant changes to the main concept, then the limitations of the current cards become a problem for massive IoT deployments. This pushes the advancement of the SIM cards and in recent years we have had major new solutions for network authentication.

Ericsson has reported a total number of mobile subscriptions in Q3 2019 being 8 billion [1], this includes all consumer and also IoT subscriptions together. On the other hand, Ericsson has stated that today there are about 1 billion cellular IoT devices online and by 2024, the number will have increased to 4.1 billion devices worldwide [2].
Because of the fast growth of cellular IoT, device manufacturers have to be able to quickly scale, build products that withstand the technology advancement but at the same time, there is a need for a scalable subscriber identity module solution.

Today, one of the bottlenecks is the lack of SMS support and SMS roaming on certain new IoT focused cellular access technologies for example, NB-IoT.

The main objective of the research is to concentrate on the following questions:

How to remotely provision the M2M eSIM without SMS support?

1) Why is there a need for a different provisioning approach?
2) Which solutions could be used and what are the benefits or drawbacks?
3) How secure is the remote M2M eSIM provisioning?
4) How secure is the SMS protocol?

The need for this paper comes from the cellular technology industry and IoT device manufacturers, who are confronted with these limitations today.

2 Background

This section will introduce the necessary background information needed for understanding the Subscriber Identity Module and its relation to the Short Message Service. Background information will also bring out differences in SIM form factors, SIM technologies and the importance of SMS for remote SIM Provisioning.

2.1 Overview of SIM cards

The Subscriber Identity Module stores subscriber registration information used to access cellular networks, parameters like ICCID, IMSI, Authentication Key's but also operator specific data like SMSC addresses and more

ICCID stands for Integrated Circuit Card ID and it is a unique value specifying a UICC or SIM card. An operator profile is associated with a particular ICCID and IMSI number.

IMSI stands for International Mobile Subscriber Identity which is a unique value for an operator profile. A regular IMSI consists of 15 digits, where the first three are Mobile Country Codes (MCC), the next two are Mobile Network Codes (MNC) and all the next digits for the Mobile Subscriber Identification Number (MSIN).

Authentication Key or Ki is used together with other parameters to authenticate the SIM on the operator’s network. This key is compared to the parameter in the operator’s Home location register (HLR).

The need for EID was introduced with the new concept of Over the Air (OTA) provisioning operator profiles on eSIM. As the ICCID and IMSI values are associated with a profile, there is now a need to identify the physical eSIM card itself, which can be done using the EID number. The EID is 32 digits long consisting of industry identifier, country code, issuer identification, issuer-specific information and check digits.

2.1.1 SIM card form factors

Today we have different form factors available, mainly differentiated by plug-in SIM or solderable SIM. Most popular being - Full Sized (1FF), Mini-SIM (2FF), Micro-SIM (3FF), Nano-SIM (4FF) and solderable SIM (MFF2), shown in Figure 1.

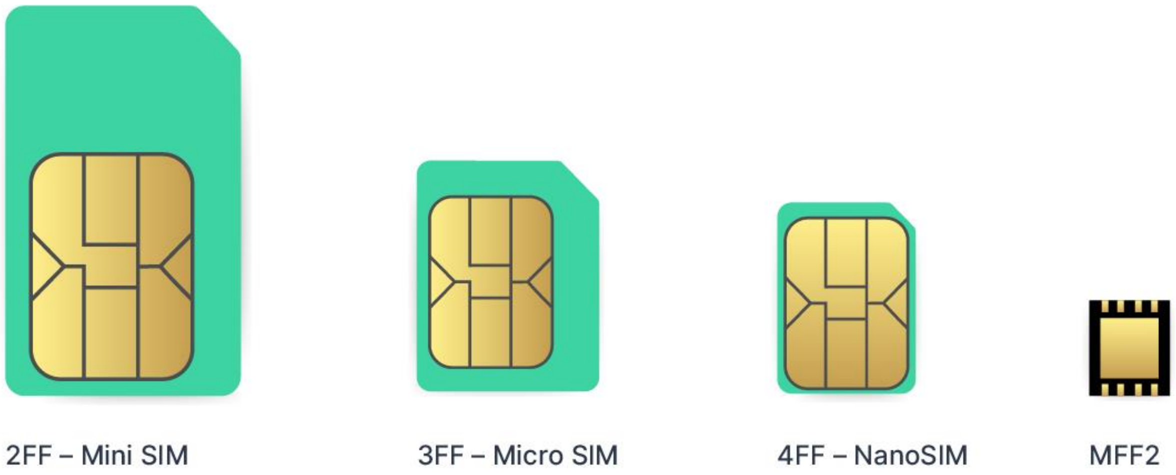


Figure 1. SIM card form factors [3].

While the form factor is just the physical layout of the SIM module, and do not always reflect the technology used. New SIM technologies have been introduced in the recent decade because of the growing need for better SIM solution in IoT devices.

The most known and promising new technology for SIM solutions is eSIM, but there are also solutions like iSIM and nuSIM in developments.

2.2 SIM technologies

eSIM or embedded SIM revolutionizes the subscriber identity module with the possibility to remotely provision new operator profiles without needing to access the SIM physically. While it is often thought that embedded SIM form factor (MFF2) is eSIM, then actually the eSIM can come in any form factor ranging from 1FF to 4FF and MFF2. The eSIM differentiates from the software running on the chip [4]. eSIM is GSMA compliant and certified solution.

iSIM or integrated SIM is a variation of eSIM. While the functionality is the same as on eUICC, iSIM is integrated directly into the cellular module’s hardware. This eliminates the need for an external component, improving device reliability, power management and reducing bill-of-materials cost [5].
It's important to note that today, the iSIM is not a standardized solution and has not been approved by GSMA.

nuSIM is specially designed for Low Power Wide Area Network (LPWAN) technologies like NB-IoT and LTE-M. The SIM has been made as simple as possible removing many functions a regular SIM, eSIM or iSIM has. SIM Toolkit, Java Card support, OTA access and other elements of SIM file structure are removed. This allows the profile size to be minimal, below 500 bytes [6]. nuSIM is lacking remote provisioning capabilities, all operator profiles need to be loaded onto the SIM during production [6]. nuSIM has not been certified by GSMA and is not a standardized interoperable solution.

This thesis will concentrate on eSIM technology as this is a GSMA certified and standardized interoperable solution. While still far behind traditional SIM cards, eSIM has the highest adoption rate in M2M compared to iSIM and nuSIM.

2.3 eSIM architecture

The business requirements for eSIM are different based on various usage models. Based on that GSMA has divided it into two different models [4]:

1) Consumer eUICC

2) M2M eUICC

This thesis is focused on the M2M model, but general knowledge and comparison of two models are required to evaluate the research problem.
The following chapters will explain the differences on a high level but also give detailed knowledge about the M2M eUICC model.

2.3.1 Consumer and M2M model

In the consumer eSIM model, a person initiates the new profile download over a Remote SIM Provisioning server called Subscription Manager - Data Preparation + (SM-DP+). The SM-DP+ handles secure storing of profiles and also routing of these to the eUICC. This can be done usually through scanning a QR code which contains a link to the correct SM-DP+, allowing to establish a secure connection to the system and proceed with the download and profile enabling. To enhance the consumer experience, a special feature called Root Discovery Service (SM-DS) has been set in place. SM-DS allows subscriptions with an agreed contract to retrieve the profile directly into the device. The device will periodically poll the SM-DS server about new profile availability. Every different operator has to have their own SM-DP+ instance and the eUICC can establish a link according to operator's different RSP servers. The SM-DP+ can also be hosted by a partner of the operator, usually an eSIM manufacturer. Once the profile has been downloaded from the SM-DP+, the user is now in control to swap the profile on their device using a Local Profile Assistant (LPA) tool.
The consumer model can be considered as a pull mode [7].

A consumer can use different access technologies to download a profile from the SM-DP+. The eUICC can come without any operator profile loaded and the consumer is responsible for establishing a connection (for example using Wi-Fi networks).

The M2M model is quite different as the profile downloads and other actions are pushed to the device remotely. The device does not anymore initiate the request itself. This is achieved with a completely different infrastructure consisting of Subscription Manager - Data Preparation (SM-DP) and Subscription Manager - Secure Routing (SM-SR) servers. The SM-DP stores the securely encrypted operator profiles, ready for over the air provisioning. An M2M eUICC is paired to one SM-SR, which can securely route SM-DP traffic to the correct eUICC. This means a M2M eUICC is always relying on the SM-SR. The owner of the SM-SR has also all the control over the eUICC. While an SM-SR swap is possible, it can be costly and involves technical configurations. Similarly to the consumer model, the operator does not need to host the SM-SR and SM-DP itself, but can also partner with an eSIM manufacturer or servie provider who leases the provided services. There is no need for LPA in M2M model, as the SM-SR is in charge of every eSIM action [8].

The M2M device needs to establish a connection to the SM-SR, this means all eUICCs need to come with a profile loaded onto it at the production, it is called a bootstrap profile. Bootstrap profiles have global coverage and are used to download the appropriate active profile.

2.3.2 M2M eSIM architecture

The technical solution used for management and provisioning of M2M eSIM ensures access for hard to reach devices. To provide an interoperable solution the architecture has been standardized in the Remote Provisioning Architecture for Embedded UICC Technical Specification [8] and shall be compliant with Embedded SIM Remote Provisioning Architecture [9].

As mentioned in section 2.3.1 the M2M model consists of two entities, Subscription Manager - Data Preparation (SM-DP) and Subscription Manager - Secure Routing (SM-SR), shown in Figure 2.

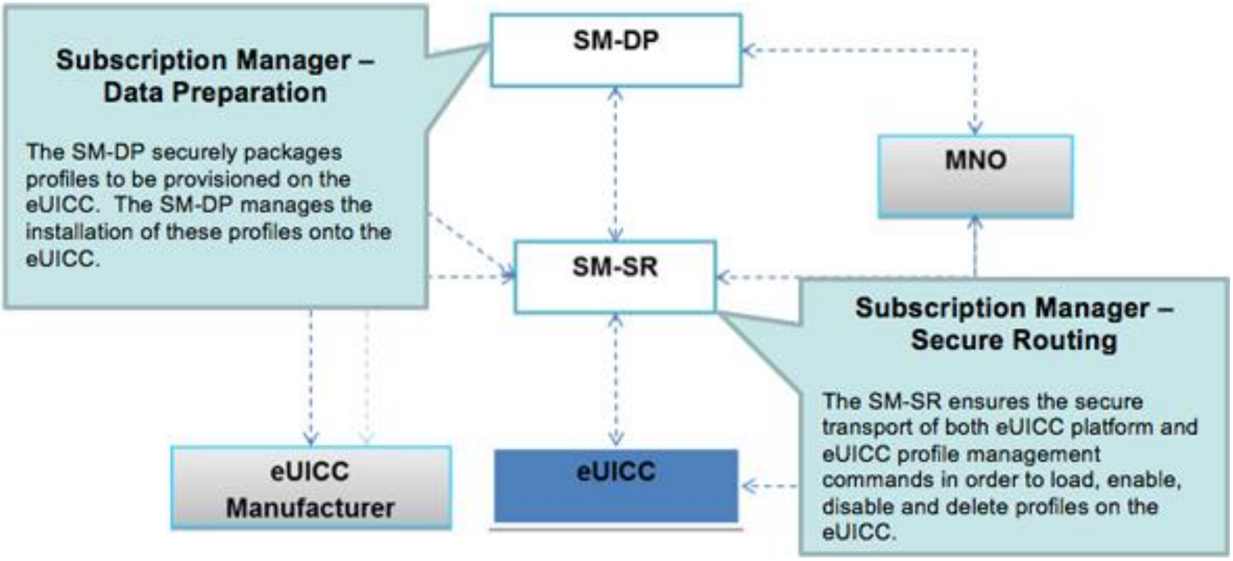

Subscription Manager – Data Preparation
The SM-DP securely packages profiles to be provisioned on the eUICC. The SM-DP manages the installation of these profiles onto the eUICC.
SM-DP
MNO
SM-SR
Subscription Manager – Secure Routing
The SM-SR ensures the secure transport of both eUICC platform and eUICC profile management commands in order to load, enable, disable and delete profiles on the eUICC.
eUICC Manufacturer
eUICC

Figure 2. Split & Roles of the GSMA Architecture's Subscription Manager [10].

Figure 3 presents the communication between the infrastructure components and the eUICC. This is divided into the following interfaces: ES1(EUM to SM-SR), ES2(MNO to SM-DP), ES3(SM-DP to SM-SR), ES4(MNO to SM-SR), ES5(SM-SR to eUICC), ES6(MNO to eUICC), ES7(SM-SR to SM-SR), ES8(SM-DP to eUICC).

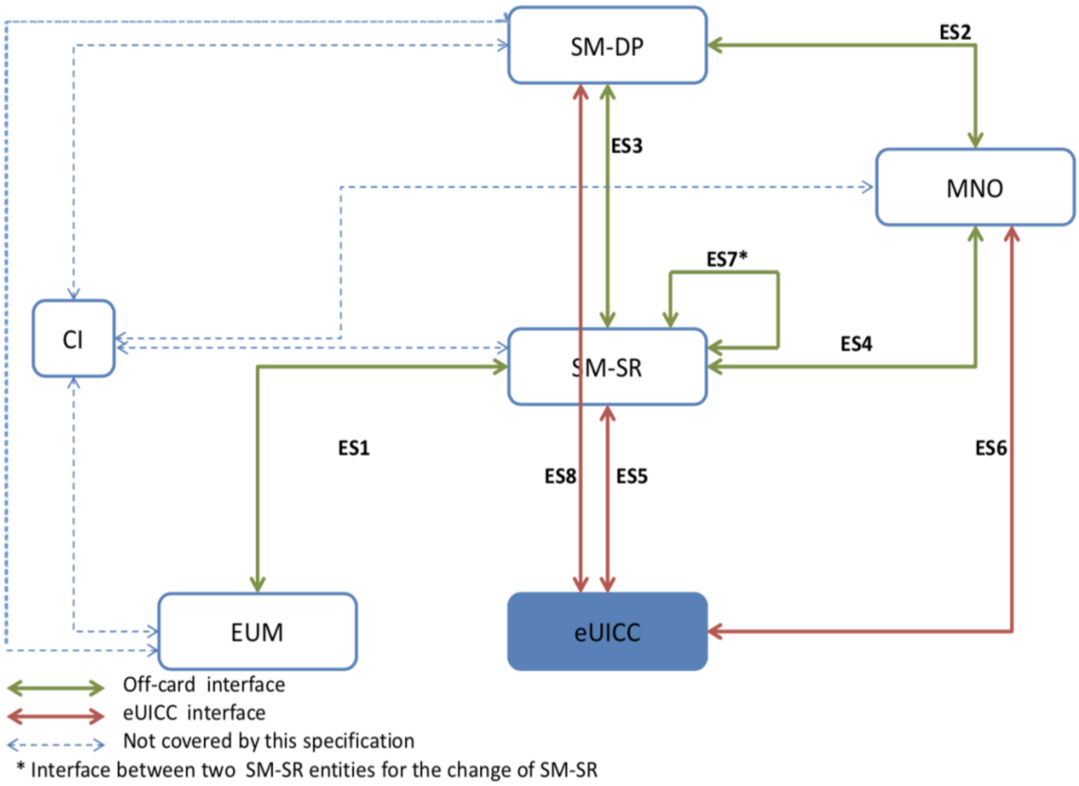

SM-DP
MNO
CI
SM-SR
EUM
eUICC
ES1
ES2
ES3
ES4
ES5
ES6
ES7*
ES8
Off-card interface
eUICC interface
Not covered by this specification
* Interface between two SM-SR entities for the change of SM-SR

Figure 3. eSIM infrastructure interfaces [11].

The work will cover eUICC interfaces ES8 and ES5, other off-card interfaces will be out of scope. Important functions of ES5 include CreateISDP, EnableProfile, DisabledProfile, DeleteProfile, eUICCCapabilityAudit, MasterDelete, SetFallbackAttribute, EstablishISDRKeySet, FinaliseISDRHandover and UpdateSMSRAddressingParameters [11]. ES8 includes DownloadAndInstallation, EstablishISDPKeySet, UpdateConnectivityParameters SCP03 functions [11]. eUICC interfaces involve the management and provisioning with the eSIM, which is handled by the SM-SR. ES8 interface (SM-DP to eUICC) cannot connect directly from the SM-DP but needs to use the secure routing functionality of SM-SR. The SM-SR can use a combination of SMS, CAT_TP and HTTPS for communication handling.

2.4 Bearer Independent Protocol (BIP)

Bearer Independent Protocol (BIP) allows high-speed IP connections to be established between the SIM and device. BIP is an essential part of Remote SIM Provisioning as the provisioning commands and profiles are sent using this communication channel.

According to GSMA set standards, BIP is one of the device function requirements with the following commands [8]:

1) OPEN CHANNEL (UDP and TCP over IP)
2) CLOSE CHANNEL
3) RECEIVE DATA
4) SEND DATA
5) GET CHANNEL STATUS
6) ENVELOPE (EVENT DOWNLOAD)

Depending on the device, BIP can be already enabled by default or might need device configuration.

2.5 Short Message Service for Remote SIM Provisioning

Short Message Service (SMS) is used for:

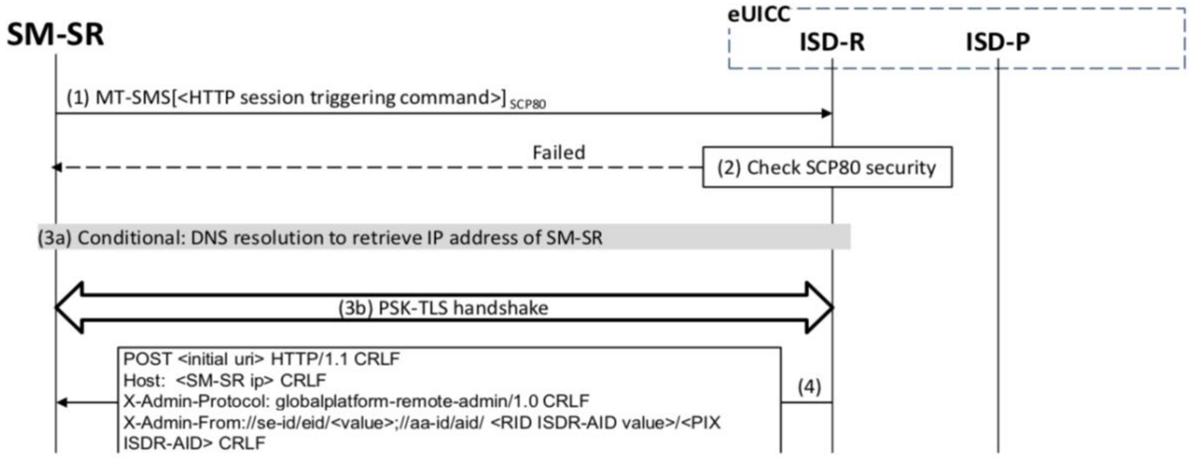
- Person to Person(P2P) communication
- Application to Person (A2P) and Person to Application (P2A) communication
- Over the Air (OTA) Remote SIM Provisioning for M2M eUICC

While the first two are common and usually familiar use cases, then the SMS need for RSP is less known.

SMS messages are routed and regulated through the Short Message Service Center (SMSC). All messages sent will include the message but also an SMSC address, which will be stored in the electrical profile of the operator. The SMSC will receive, route to the destination and when needed store the message.

GSMA SGP .02 documents that SM-SR has to use binary SMS for initiating the HTTPS session [8]. SM-SR has to have a link established with a responsible SMSC to forward provisioning messages. The binary SMS (SMS-PP) will be addressed to the eUICC ISD-

R with instruction to open the Bearer Independent Protocol channel and create a TLS socket, shown in Figure 4.


SM-SR
eUICC
ISD-R
ISD-P
(1) MT-SMS[<HTTP session triggering command>] SCP80
Failed
(2) Check SCP80 security
(3a) Conditional: DNS resolution to retrieve IP address of SM-SR
(3b) PSK-TLS handshake
(4)

```
POST <initial uri> HTTP/1.1 CRLF
Host:  <SM-SR ip> CRLF
X-Admin-Protocol: globalplatform-remote-admin/1.0 CRLF
X-Admin-From://se-id/eid/<value>;//aa-id/aid/ <RID ISDR-AID value>/<PIX
ISDR-AID> CRLF
```

Figure 4. Sequence for HTTP session triggering [8].

SMS can be divided based on the message direction:

- SMS Mobile Originating (MO)
- SMS Mobile Terminating (MT)

All device initiated or outbound messages are considered as Mobile Originating (MO). All received or inbound messages are Mobile Terminating (MT). RSP platform will forward the trigger for opening the BIP channel through an SMS-MT to the eUICC. Therefore SMS-MT is a requirement to establish ES5 and ES8 interface connections.

2.5.1 SMS availability

SMS-MT and SMS-MO availability depend on cellular hardware, cellular networks and SMS roaming agreements.

While consumer subscribers can until today enjoy SMS worldwide without any restrictions, IoT subscription plans of operators most often do not include voice and SMS anymore. Also roaming deals worldwide have a separation between data roaming, voice roaming and SMS roaming, where for IoT subscriptions not in every country you will get SMS roaming support. While this restriction is mostly commercially motivated and from the technical side also IoT subscriptions could have SMS enabled, there are network technologies where SMS is not available from the technical viewpoint.

New Low Power Wide Area networks like Narrowband IoT (NB- IoT) do not support SMS by default. GSMA NB-IoT Deployment Guide states that only some operators worldwide deploying NB-IoT will support SMS and therefore no clear deployment recommendations are given at the time. SMS is not included in the key minimum features of NB-IoT. Operators try to keep their costs to a minimum with the NB-IoT networks [12].

Without at least binary SMS-MT support, eSIM provisioning will not be possible.

3 eSIM Trace

This paragraph will analyze the GSMA M2M eSIM solution that is based on SGP.02 specification. To analyze the communication of a SIM card there are mainly two possibilities. Either a network level trace or a trace between the SIM card and device. While both have benefits and drawbacks for the results, the network level trace needs more dedicated hardware and is much more expensive to set up.

In this research, we are going to use the method of tracing the communication between the eSIM card and cellular module.

3.1 Tracing tools

The tool which traces the communication needs to be capable of reading the communication protocols used to transfer information between the cellular module and the eSIM card. Application Protocol Data Unit (APDU) commands are exchanged between the device and card, these commands can be decoded, translated and analyzed.

The choice of tracers capable of APDU sniffing is limited. While there are a few more options, three popular devices are:

1) UL Mobile Security SmartConnect 3

2) Comprion MiniMove

3) Osmocom SIMTrace 2

All three devices are able to trace APDU commands, but the supported protocols are different. SIMTrace 2 supports T=0 and T=1 protocol but does not support the Bearer Independent Protocol.

The Comprion and UL tools are capable of showing raw data in form of APDUs but also have the possibility to translate raw data according to ETSI TS 102 221 v12.0.0 [13] and

3GPP TS 31.102 v12.6.0 [14]. With the correct card keys, it will be possible to decrypt the communication. In this research, the UL Mobile Security SmartConnect will be used to trace communication.

3.2 Cellular hardware

As this thesis concentrates on IoT and M2M eSIM solutions it is also advised to use cellular hardware that is specific for M2M. A consumer handset has software implementations to execute and handle certain commands or situations. To minimize affecting variables the use of a consumer handset is not ideal.

In the experiment, an IoT cellular module will be used, which has direct AT-command interface access. An evaluation or development kit provides USB COM-port interfaces, AT-command interface and also hardware level debugging capabilities. uBlox EVK together with a 3G cellular interface board uBlox SARA-U201 will suit the scope of the test.

3.3 Tracing eSIM transactions

We set up the UL SmartConnect tool between the eSIM card and the uBlox cellular module. The cellular module configured with AT-commands to have SIM ToolKit and BIP support enabled. For this trace, we will be using 1oT's plastic eSIM card. The trace log is included in Appendix 1 – eSIM trace Translated view.

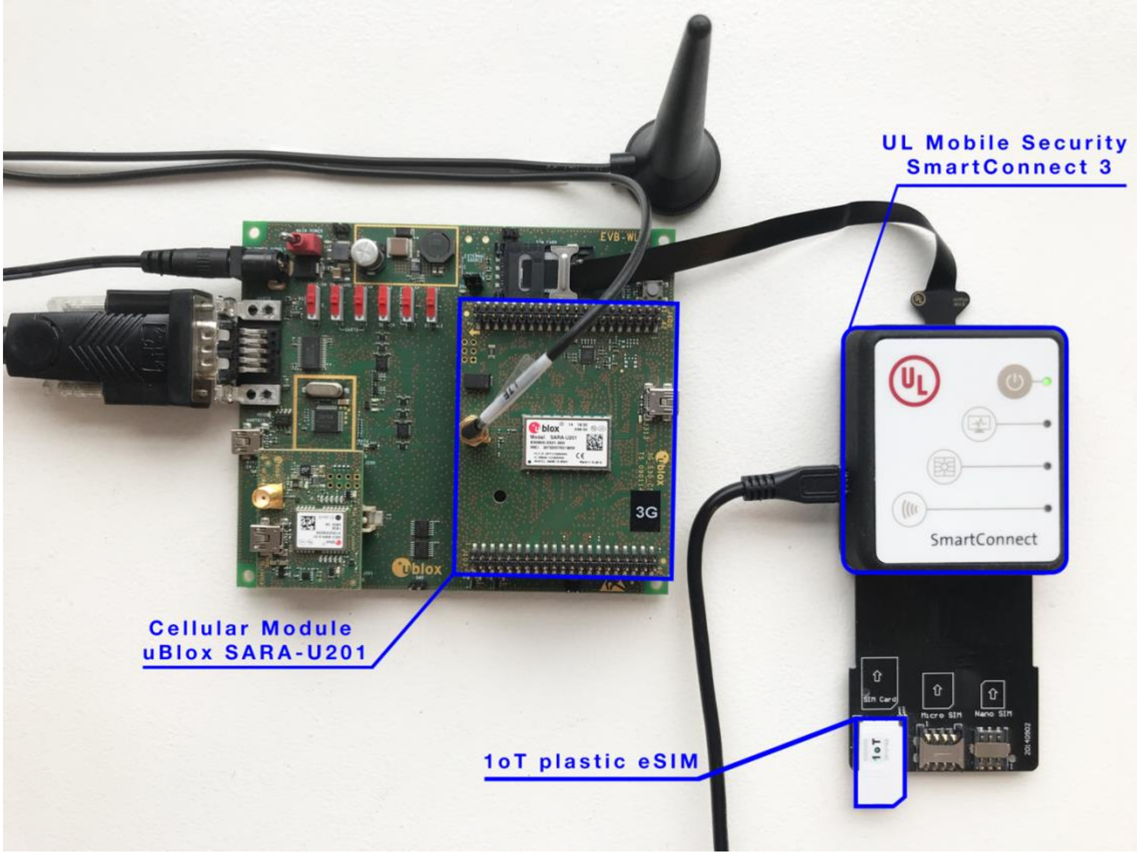
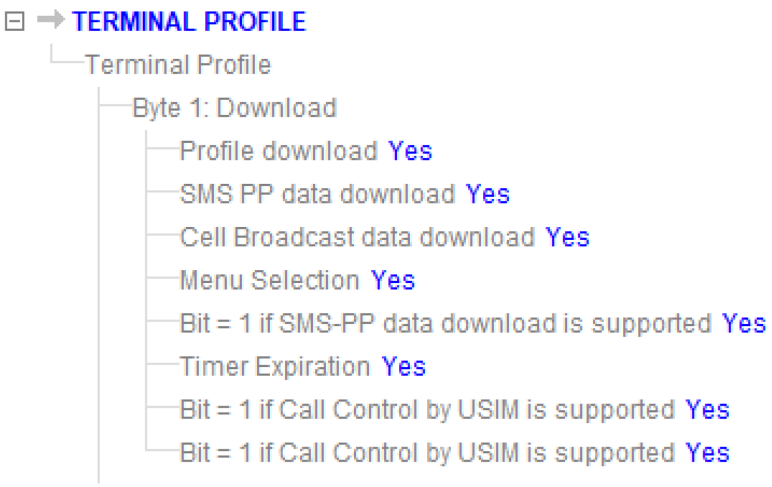


Figure 5. Setup for tracing eSIM card.

Powering up the device, the first bytes of data exchanged between the eUICC and device is ANSWER TO RESET (ATR). An ATR message contains information about the eSIM card capabilities, card communication parameters and card state.

TERMINAL PROFILE is another essential data exchange the trace should focus on. It includes information about device capabilities and functionality. Byte 1 shows if SMS-PP data download is supported, SMS-PP is the same push MT-SMS used to initiate the eSIM management. Byte 1 confirms that our cellular module, uBlox SARA-U201 supports eSIM profile download. To confirm this we have a look at Byte 12, which shows the support of Bearer Independent Protocol. BIP commands listed in section 2.4 need to be supported by the hardware.

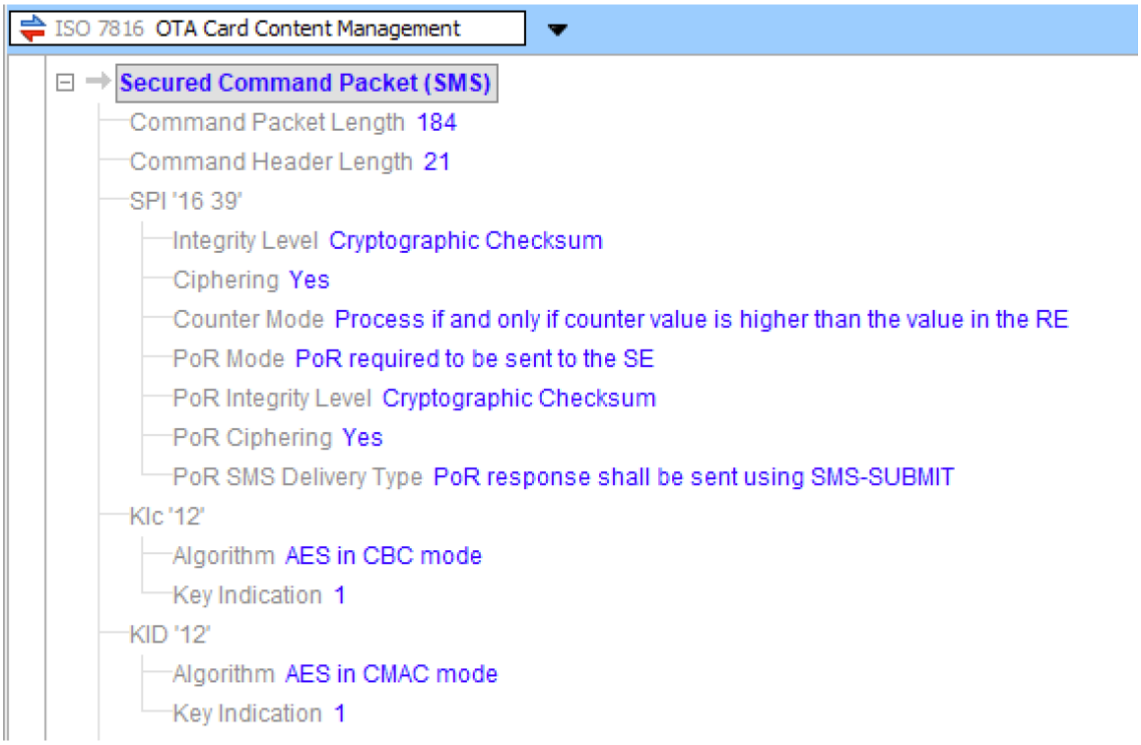


```
TERMINAL PROFILE
  Terminal Profile
    Byte 1: Download
      Profile download Yes
      SMS PP data download Yes
      Cell Broadcast data download Yes
      Menu Selection Yes
      Bit = 1 if SMS-PP data download is supported Yes
      Timer Expiration Yes
      Bit = 1 if Call Control by USIM is supported Yes
      Bit = 1 if Call Control by USIM is supported Yes
```

Figure 6. TERMINAL PROFILE Byte 1.

We will initiate the download profile, an ES8 DownloadAndInstallation call between the eUICC and SM-DP, from 1oT's eSIM infrastructure. According to the SGP.02 specification and Figure 4 we should see the binary MT-SMS push dedicated to the eUICC to initiate the profile download.

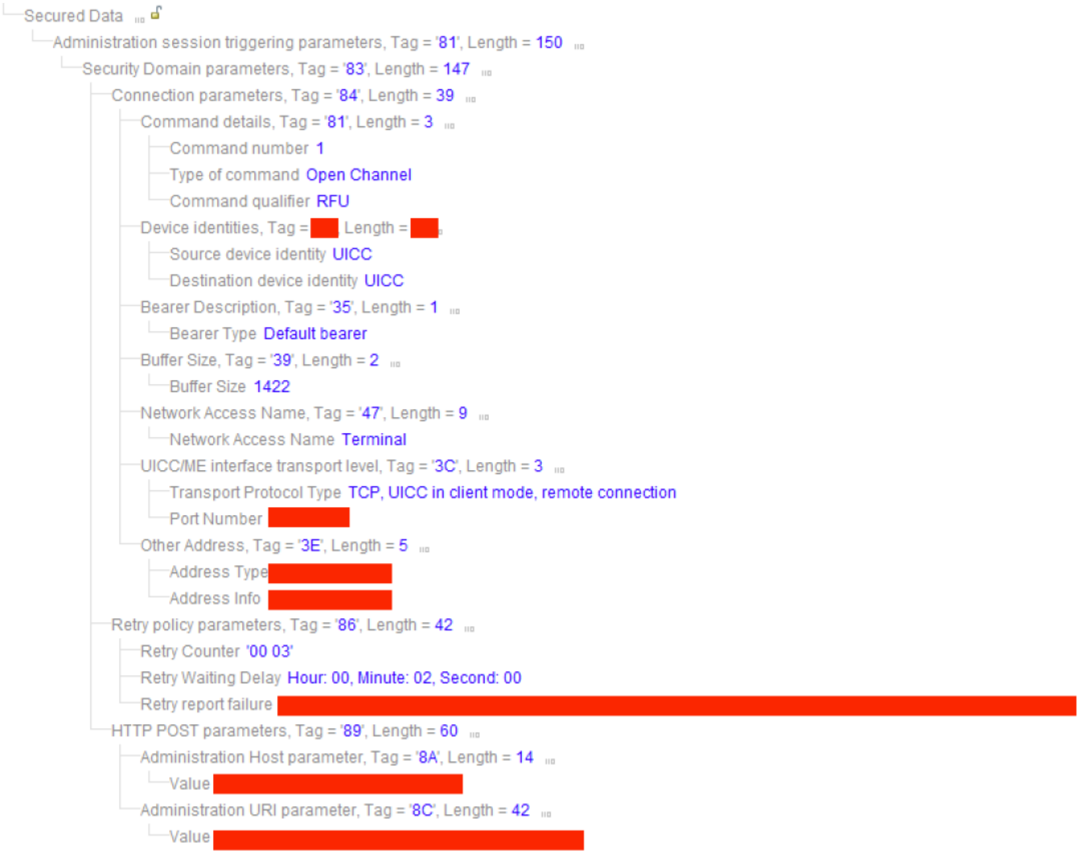
The SMS push consists of two ENVELOPE SMS-PP data download messages. After the Secure Parameter Index/Indicator (SPI) header we can see that two different algorithms are used for data protection. KIc, indicating the key and algorithm for ciphering, uses the AES algorithm in CBC (Cipher Block Chaining) mode, KID, indicating the key and algorithm for integrity protection, uses the AES algorithm in CMAC (Cipher-based Message Authentication Code) mode. These key parameters are confidential and in the wrong hands could be used for malicious activities, therefore operators do not share them with subscribers. In our testing, we are using a test eSIM card, which 1oT provided the keys for. When deciphering the content with KIc and KID we will be able to inspect the parameters of the secure data.



```
ISO 7816  OTA Card Content Management
  Secured Command Packet (SMS)
    Command Packet Length  184
    Command Header Length  21
    SPI '16 39'
      Integrity Level  Cryptographic Checksum
      Ciphering  Yes
      Counter Mode  Process if and only if counter value is higher than the value in the RE
      PoR Mode  PoR required to be sent to the SE
      PoR Integrity Level  Cryptographic Checksum
      PoR Ciphering  Yes
      PoR SMS Delivery Type  PoR response shall be sent using SMS-SUBMIT
    KIc '12'
      Algorithm  AES in CBC mode
      Key Indication  1
    KID '12'
      Algorithm  AES in CMAC mode
      Key Indication  1
```

Figure 7. eSIM trace KIc and KID cryptographic algorithms.

We can see that the SMS-PP or SMS push message does contain the command with instructions to open a BIP channel to the eSIM infrastructure servers. The secure data part of the message comes with HTTP POST parameters like server IP address and URI, which the eSIM card will use for opening the BIP channel.



```
Secured Data
  Administration session triggering parameters, Tag = '81', Length = 150
    Security Domain parameters, Tag = '83', Length = 147
      Connection parameters, Tag = '84', Length = 39
        Command details, Tag = '81', Length = 3
          Command number 1
          Type of command Open Channel
          Command qualifier RFU
        Device identities, Tag = [redacted] Length = [redacted]
          Source device identity UICC
          Destination device identity UICC
        Bearer Description, Tag = '35', Length = 1
          Bearer Type Default bearer
        Buffer Size, Tag = '39', Length = 2
          Buffer Size 1422
        Network Access Name, Tag = '47', Length = 9
          Network Access Name Terminal
        UICC/ME interface transport level, Tag = '3C', Length = 3
          Transport Protocol Type TCP, UICC in client mode, remote connection
          Port Number [redacted]
        Other Address, Tag = '3E', Length = 5
          Address Type [redacted]
          Address Info [redacted]
      Retry policy parameters, Tag = '86', Length = 42
        Retry Counter '00 03'
        Retry Waiting Delay Hour: 00, Minute: 02, Second: 00
        Retry report failure [redacted]
      HTTP POST parameters, Tag = '89', Length = 60
        Administration Host parameter, Tag = '8A', Length = 14
          Value [redacted]
        Administration URI parameter, Tag = '8C', Length = 42
          Value [redacted]
```

Figure 8. eSIM trace Secure Data parameters.

The eSIM management commands ES5 and ES8 calls will be sent over the HTTP data channel after the secure PSK-TLS handshake has been performed which provides data encapsulation, not over SMS.

From the conducted eSIM trace we can verify that the SMS payload includes the command to open a BIP channel and the needed HTTP POST information like IP address, port number and URI. These parameters are needed to open the BIP channel to the SM-SR of this particular eSIM. Once the BIP channel is open, the SM-SR can provide the profile or transaction information of an SM-DP. If these parameters with the open channel command can be delivered to the eUICC with other services than SMS, there would be minimal change to the existing infrastructure and remote provisioning process in general.

Enable, disable and delete actions were also traced and analyzed. The SMS push content is the same, requesting to open a BIP channel with the correct server destination parameters. Appendix 2 – eSIM trace OTA Card Content Management viewcontains the OTA Card Content Management trace view of the incoming SMS for the entire trace.

4 Solutions

This chapter will look into the possible solutions to remotely provision eSIM without using SMS support. The solutions are theoretical but based on today’s technical possibilities. While these solutions are out of the GSMA standard, they could be considered in new versions of the specification to improve the scalability and security of M2M remote SIM provisioning.

4.1 Solution 1 - Polling applet

4.1.1 Java Card applets

Java Card enables to host and run Java technology on resource constraint device like smart cards and SIM cards.

The Java Card platform allows applications to manage network communication themselves, allowing initiating of client communication with off-card entities. Supported protocols include TCP, UDP, HTTP, HTTPS and TLS [15].

Popular Java Card applets used on SIM and eSIM cards include IMEI lock, SIM health reporting, Quality of Service reporting, Geofencing and more.

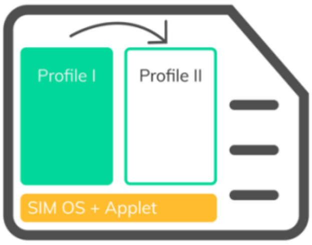
There are no hardware requirements the IoT device to support and run an applet, the host of the applet is the eSIM itself. Hardware requirements come into place only when the applet is performing actions outside of the secure element of the SIM and needs to communicate with the hardware. In this case, this is achieved with SIM Application Toolkit commands which most devices support.

4.1.2 Hosting an applet

An applet can be stored in different memory allocations on the eSIM card, two mainly used solutions are:

- SIM operating system level
- Profile level

Applets stored together with the SIM operating system (OS) provide resilience to effects caused by eSIM profile changes. The applet will be always accessible independent of which profile is currently enabled. This approach can also be considered as an extension of the OS.



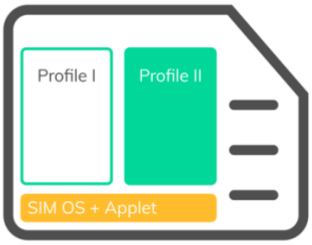
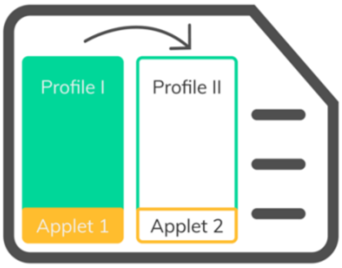


Figure 9. SIM operating system level applet [16].

Profile level applets are stored in the Secure Domain (SD) of the currently active profile. This makes it dependent on the profile, with a profile swap the applet becomes unavailable. While the applet could be implemented on only these operator profiles which are in a need for it, there would be technical problems of controlling the applet while the profile swaps are conducted.



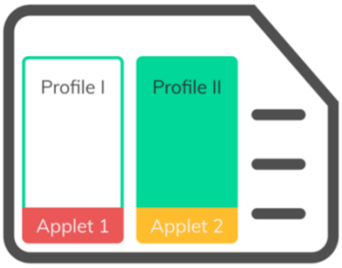


Figure 10. Profile level applet [16].

4.1.3 Polling applet

The concept of solution 1, the polling applet, involves a Java Card applet that will trigger a BIP channel from the device itself to the controlling SM-SR. This step is also usually done after the SMS-PP is received, but in case of a polling applet, there will be no need for an SMS-PP which initiates the action. The applet will initiate the opening of the BIP channel itself after a certain time frame, it can be configured to do it in minutes, hours, days. The parameters which were passed with the SMS-PP (IP address, port number, URI) need to be predefined at the time of production or installing of the applet. The applet should be stored on the OS level, to avoid problems while switching operator profiles.

On the server side, some changes will need to be implemented to support this approach. All actions dedicated to an eSIM need to be queued until the SIM itself establishes a connection and the BIP channel is opened.

To improve usability, the new parameter for setting the polling interval should be passed through the BIP channel back to the device. This will enable us to change or specify the polling interval to suit different IoT projects.

The applet will open the channel after every reset to the SIM and start the timer interval over again. In some cases, only polling after a restart might even be enough and it would help to overcome the applet's drawbacks.

4.1.4 Drawbacks

The polling applet comes with two drawbacks compared to the SMS-PP based solution.

Firstly, it will increase data consumption. Likely most of the polling intervals or opened channels will be to check the server queue without having any bending actions to complete. Over the years of usage, this small data amount can pile up to a considerable consumption over time.

Secondly, the applet will affect the power consumption of the SIM. As with the data consumption, this would be very minimal. There are no recent studies that document the possible extra power consumption that applets might have and without further investigation, it is hard to tell how big of an impact it would be.

4.1.5 Conclusion

Most likely an environmental sensor which reports measurements a few times a day does not need daily switching of operator profiles. More important to this sensor is the ability to use LPWAN networks like NB-IoT which might not support SMS. Therefore, the polling applet ideally fits the need for many IoT projects which are not moving devices and where the environment does not change often.

4.2 Solution 2 - Remote LPA for M2M applications

Local Profile Assistant (LPA) is part of the GSMA eUICC consumer specification, the M2M model does not use this feature. This section will present the possibility of adopting the consumer model for IoT use-cases while not being dependent on SMS support. The main conceptual difference between the two models is that the M2M model uses push mode and consumer pull mode. If we adapt the consumer model for IoT, we will need to preserve the capabilities of remotely managing the profiles, without the intervention from the end-user. Solution 2 is conceptually different as it will not be based on the M2M infrastructure, but the end goal to provide M2M device remote eSIM management capabilities remains the same.

4.2.1 Local Profile Assistant (LPA)

The Local Profile Assistant is responsible for the download and installation of encrypted operator profiles, while also providing local management possibilities for the end-user. LPA provides three separate functions - Local User Interface (LUI), Local Profile Download (LPD) and Local Discovery Service (LDS). LUI allows the end-user to perform management of local profiles. LPD handles the profile download and transfer of the downloaded profile into the eUICC. LDS is responsible for interaction with SM-DS and retrieving of events.

LPA can exist in the device or in the eUICC. If the LPA is provided by the eUICC another function called LPA service is used as a layer between device and eUICC. More often the LPA is on the device and communicates with ES interfaces to the eUICC.

4.2.2 Remote management of LPA

If the LPA could be remotely managed it would provide means for the consumer model to be applicable also for IoT devices, while still being for most parts compliant with the GSMA specification and involve only moderate technical changes to the core protocol.

Currently, the industry is looking towards using SM-DP+ also for IoT use-cases, as using one infrastructure for IoT and consumers would lower costs for operators and ease the maintenance. eSIM vendors like Giesecke+Devrient, IDEMIA or Thales are currently frontrunners and looking into ways this could be achieved. It's still unclear how it would be possible to remotely manage the LPA but most likely it would be done on the device

LPA, because devices are not as resource constraint as the eUICC itself. This would mean specific software running on a device that could also talk to the specific LPA running on the device. OTA management would be based on IP connectivity.

4.2.3 Security concerns

While the GSMA has made sure that the consumer and also M2M specifications are secure and no unauthorized management of profiles can happen, this kind of modification to the LPA raises security risks.

If the remotely manageable LPA is located on the device side, weak security measures are easy to become a reality which will affect the whole chain of provisioning and management for this devices eSIM.

4.2.4 Conclusion

The technical side of remotely managing LPA is still unclear, but the benefits of achieving this are big. Operators could adopt one infrastructure for consumer and IoT, support for SMS would not be needed.

Even though the LPA can be also hosted on the eUICC itself, it's not a common approach today. If there is also any remote management of the LPA, this would need to be done on the device LPA side as eUICC chips are very resource constraint and it would involve heavy changes to the specification. Remote LPA will be a hardware specific solution, relying on hardware manufacturers to implement these supports.

4.3 Solution 3 - Fixed IP SIM card

With the explosion of devices connected to the internet, public IPv4 addresses have become scarce. Mobile operators use Network Address Translation (NAT) to serve multiple devices under one public IP. While it helps to solve the problems of limited public IP addresses, this together with implemented firewalls prevent direct access to the device or SIM card. This is why the current GSMA M2M eUICC specification uses the phone number, technically known as MSISDN, instead of IP address to establish the connection to the device. MSISDNs are fixed to a profile and known to the SM-SR throughout the lifecycle of the eSIM. This section will look into using IP connectivity for transaction initialization and data download.

4.3.1 eSIM card with a public fixed IP address

Even as fixed IPv4 addresses are scarce there is still the possibility of requesting a SIM card which will have a public fixed IP address. This will allow two-way communication and enable the eSIM infrastructure to know always exactly the destination for communicating with the eSIM.

But fixed IP SIM cards are costly and not a scalable solution that could be standardized and used throughout the whole eSIM ecosystem. It would be a solution for very limited use-cases, for example, critical infrastructure sector. Public IPs involve security risks as the address will be visible to everyone. Potential malicious acts against IoT devices include denial of service, battery drain and data consumption drain [17].

4.3.2 eSIM card with a private fixed IP address

The second possibility to know the IP destination of a SIM would be to use a private Access Point Name (APN) with fix private IP address. An APN is a gateway which provides a point of entry onto an IP network. Private APN is only accessible for the SIM subscription owner, to establish a connection to the eSIM, you need to have access to the private APN. This gives an extra layer of security and control, but also means that the SM-SR would need to be integrated with each of these Private APNs.

4.3.3 Complications

The public fixed IP address or private APN is set up and established with one operator. If you leverage the eSIM functionality and change the operator you would lose the previous setup.

If the new operator also provides a public fixed IP, it will not be the same public fixed IP address, so the provisioning infrastructure needs to know the new IP address coming with the profile. Similarly, as currently, the eSIM infrastructure knows the MSISDN of the new profile.

But establishing a new private APN configuration between the eSIM infrastructure and new operator is a manual process and involves even further setup costs.

If large corporations want to mitigate risk, it would be a viable solution for them. One example being millions of smart water meters, if an operator switches off this a radio access technology, this overhand process would be appropriate.

4.3.4 Conclusion

Using IP connectivity would seem like a logical step in the world full of IoT devices and data being the only connectivity channel needed, but it involves many challenges as of today. Public fixed IP SIM cards cannot be used for every device as they involve higher costs and come with security concerns.

Using private fixed IP addresses with a private APN is a right solution once you have enough of devices where the setup is cost effective.

4.4 Solutions comparison

Table 1 compares the polling applet, remote LPA for M2M applications and fixed IP SIM card solutions.

	Solution 1 - Polling Applet	**Solution 2 - Remote LPA for M2M applications**	**Solution 3 - Fixed IP SIM card**
Difficulty of implementation	Easy	Difficult	Difficult
Cost of implementation	Low	Low	High
Scalability	Scalable	Medium scalability	Not scalable
Hardware support required	No	Yes	No

Interoperability between eSIM infrastructures	Yes possible	Yes	Hard to achieve
Security concerns	Low security risk	High security risk	Medium security risk
Delay in transaction	Dependent on the poll interval	Immediate push	Immediate push
Use-case	All IoT use-cases	Specific use-cases	Specific use-cases
Compliant with GSMA specification	No (minimal changes to the specification needed)	No (moderate changes to the specification needed)	No (extensive changes to the specification needed)

Table 1. Comparison between solutions.

Table 1 illustrates and gives a high-level overview of the advantages and disadvantages of the three proposed solutions. Solution 1, which is using a polling applet to identify new transactions requires the least efforts for implementation. Applets are already standard products on SIM cards and have been used for various other services, making Java Card applets an ideal platform for solution 1. Implementation of solutions 2 and 3 need more customization of the eSIM specification. Keeping costs low is necessary for operators therefore solutions 1 and 2 are more suitable, while solution 3 involves the high cost of public IP addresses or setup of private APN's. The latter is also the reason why solution 3 is not as scalable to millions of subscriptions as a polling applet or remote LPA. Remote LPA is scalable as long as the hardware manufacturers support it, solution 1 and 3 are not dependent on hardware. The only solution being interoperable between different eSIM infrastructures is solution 2, because it relies on consumer specification and software on the device. Software on a device comes with higher security risks than a secure chip like an eSIM, this needs to be considered for remote LPA. Polling, dependent on the configuration, will cause delays in performing transactions, compared to push, which is used for solutions 2 and 3. Polling applet will likely fit all IoT use-cases, while remote

LPA and fixed IP SIM cards are more specific to a certain use-case, for example, critical infrastructure. In the end, all proposed solutions are not compliant with the current GSMA specification. The polling applet will need minimal change, remote LPA moderate change and fixed IP SIM cards extensive change to the current specification.

5 Security

From the beginning onwards, GSMA has developed the eSIM to provide at least the same amount of security as a regular SIM. The remote provisioning and management involve challenges to achieve this. GSMA has identified as the key risks the following [11]:

- Many parties are involved in eSIM profile management
- Profiles are not fixed to one card anymore, they can be replaced
- At the same time, there may be several profiles on one card
- eSIM management is controlled through rules and commands
- Remote provisioning and management

5.1 Remote SIM provisioning security

5.1.1 Clustering of eSIM architecture

The eSIM architecture has been built up on a clustering effect where the architecture is segmented into different security realms. The administrative entity is in charge of setting the security realm approach, based on the commercial but also regulatory impact. eUICC, eUICC manufacturer, MNO, SM-DP and SM-SR are considered as possible realms. While the realm setting can differ, the eUICC is always considered as an independent security realm.

The specification has also set of different security requirements, which can be divided into general security requirements, security requirements attached to a security realm and security requirements attached to a particular role (eUICC, SM-DP, SM-SR, M2M device).

5.1.2 eSIM cryptographic algorithms and key lengths

M2M eSIM uses a combination of cryptographic algorithms and hash methods to provide extensive security to SGP.02 specification. All cryptographic solutions need to be compliant with at least the recommendations stated in NIST SP800-57 [18]. The used algorithms, hash functions and key lengths are [8]:

- Advanced Encryption Standard (AES) - 128 bits, block size of 128 bits
- Rivest–Shamir–Adleman (RSA) - 3070bits
- Elliptic curve (ECC) - 256 bits
- SHA-256

5.1.3 Secure Channel Protocol

Secure Channel Protocol (SCP) serves the secure communication between the eUICC and eSIM infrastructure, providing confidentiality of messages exchanged. The M2M eUICC specification relies on SCP03, SCP80 and SCP81 protocols. ES5 calls use SCP80 or SCP81 protocol, ES8 calls use SCP03 as it is the only protocol that complies with requirements mentioned in section 5.1.2 [11]. All communication to the eSIM is handled by the SM-SR which means first an SCP80 or SCP81 tunnel is established (ES5 use), only then SCP03 tunnels(for ES8 use) can be opened up on top [11].

5.1.4 Security Domains

SIM cards, eSIM cards and smart cards, in general, rely on a concept called Security Domain. Security Domains are special applications having specific privileges, containing specific keys with cryptographic algorithms and conducting a specific task. The goal is to have a good role separation and data isolation. A security domain on the eUICC represents and off-card entity in the eUICC architecture. The three security domains used for eSIM platform and profile management are [8]:

- ISD-R, representative of SM-SR
  Manages ISD-P's, is installed at manufacturing time.

- ISD-P, representative of SM-DP
  Hosts one profile, contains all connectivity parameters for that profile, can be loaded OTA.

- ECASD, representative of CI
  Responsible for key set establishments, only ISD-R and ISD-P shall be able to use ECASD services, is installed at manufacturing time.

5.2 SMS Security

GSMA has identified security issues with the SMS protocol in itself but SMS is also an enabler to perform attacks using SIM card vulnerabilities like S@T SIM Jacker Exploit and WIB Vulnerability.

Security Research Labs has gathered statistics about the popularity of S@T and WIB applet on SIM cards, they measured a collection of 800 different types of SIM cards from various vendors. The research found that at least about 10,7% of SIM cards have the WIB applet installed and out of this 3,5% were vulnerable. 9.4% of the SIMs had S@T applet installed and out of this section, a subset of 5,6% were affected [19].

The next section will look into why the disabling of SMS will lower the maintenance cost for operators and improve security.

5.2.1 SMS vulnerabilities

Today SMS is a trusted enabler to exchange messages but with recent vulnerabilities found in Signaling System 7, the trust has been challenged. Documented in GSMA PRD IR.70 [20] are five cases in which fraud can happen. These cases are not dedicated attacks against the IoT device but the SMS infrastructure in general and the end-user. But some can affect the IoT device also. Five cases are:

- Spamming case
- Flooding case
- Faking case
- Spoofing case
- GT scanning

Faking, spoofing and GT scanning involves technical manipulations of the SMS core protocol and infrastructure, often to be able to send free of charge messages. The spamming and flooding cases do not involve any technical aspects. These are mostly attacks against end-users to conduct fraud. But in some cases, flooding of SMS messages to a dedicated IoT device can overwhelm the processes of the machine and result in a denial of service attack [21].

5.2.2 Simjacker exploit

Simjacker exploit has been fixed since 2013 by many vendors and most of newer SIMs are protected against it. But there are still SIM cards that do not follow GSMA standards and can be affected, these non-certified SIM and eSIM solutions are mostly used in Asia, Mexico and Columbia.

Simjacker exploit uses binary OTA messages that are sent to the device using a SIM card with a vulnerable S@T Browser on it. The SMS includes SIM ToolKit commands which are executed and run on the SIM. Similarly to the binary SMS used in eSIM management, it will be handled without the acknowledgment of the receiving device/user. The results of SIM ToolKit command execution can then be sent back to the attacker using another binary SMS. SIM ToolKit commands can provide location information, send short messages, play tones and more [22].

The conditions that need to be satisfied on a SIM card for a successful attack are:

- S@T Browser with Minimum Security Level (MSL)
- Network support for binary SMS
- Proactive SIM and Data Download via SMS-PP

5.2.3 WIB vulnerability

Ginno Security Lab is a non-profit organization consisting of security researchers who found the Wireless Internet Browser (WIB) vulnerability in 2015. The vulnerability was not published until 2019 to protect the significant number of affected end-users.

Wireless Internet Browser (WIB) is a SIM Toolkit application allowing dynamic menus to provide value-added services to the subscriber. This is done through OTA messages that are controlled by a central server.

The concept of the attack is similar to Simjacker, just executed in another environment on the cards. The exploit consists of the following steps:

1) Sending an OTA binary SMS to the affected SIM containing a WIB command.
2) WIB commands will be forwarded to the WIB applet
3) WIB applet executes the command. The command can involve further communication between the SIM and the device.
4) The WIB applet can send the command responses to a designated destination via SMS.

Similarly to SIMJacker, the WIB commands that can be executed include sending short messages, providing location information, setting up calls, playing tones, opening bearer channels and many more [23].

Information that can be retrieved using WIB exploit provides an excellent resource to target IoT devices. Either getting a location of the asset tracking device or setting up calls for eavesdropping are both only two of the severe attacks that can be conducted.

5.3 Security conclusion

Until today there are no known security breaches to the M2M eSIM specification. The core structure of eSIM leveraging on clustering and well-established functions can be considered secure. Security domains and cryptographic algorithms have been implemented already for years and extensive penetration testing of these has been conducted.

SMS functionality itself has few flaws in it, mostly leveraging on social engineering attacks which is something you can't execute against an IoT device. But SMS flooding causing denial of service and SMS being an enabler for Simjacker and WIB vulnerabilities weaken the cellular network infrastructure.

6 Summary

This thesis analyses the importance of SMS in M2M remote SIM provisioning architecture. It points out the limitations and shortcomings of the SMS protocol. The propose of this thesis is to provide solutions and improvement possibilities for the existing infrastructure.

The current solution using SMS is a bottleneck for large scale IoT eSIM deployments. Network technologies like NB-IoT, which are specially designed for IoT devices, don't support SMS services. IoT subscriptions and international roaming agreements don't include voice and SMS. This inhibits the global and large scale use of M2M eSIM which leverages on SMS.

The analyses are done based on tracing an eSIM transaction with dedicated spy hardware. An IoT cellular module with a global connectivity M2M eSIM is used. The eSIM transaction is performed and the incoming SMS is analyzed based on the trace.

The thesis proposes three different approaches to initiate the eSIM transaction without relying on the use of the SMS protocol. These solutions are described and compared based on factors like implementation possibilities, cost, scalability and more.

Throughout the thesis security of remote SIM provisioning, SMS and proposed solutions are taken into account and evaluated. Vulnerabilities based on SMS protocol are presented.

References

[1] Ericsson, "Ericsson Mobility Report," November 2019. [Online]. Available: https://www.ericsson.com/4acd7e/assets/local/mobility-report/documents/2019/emr-november-2019.pdf. [Accessed 1 December 2019].

[2] Ericsson, "Cellular IoT Evolution for Industry Digitalization," January 2019. [Online]. Available: https://www.ericsson.com/assets/local/publications/white-papers/wp_evolving-iot-forindustrialdig.pdf. [Accessed 2 December 2019].

[3] 1oT, [Online]. Available: https://1ot.com. [Accessed 3 April 2020].

[4] GSM Association, March 2018. [Online]. Available: https://www.gsma.com/esim/wp-content/uploads/2018/12/esim-whitepaper.pdf. [Accessed 3 December 2019].

[5] ARM Ltd., February 2019. [Online]. Available: https://learn.arm.com/rs/714-XIJ-402/images/Kigen-Unlocking_whitepaper.pdf. [Accessed 3 December 2019].

[6] Deutsche Telekom AG, February 2019. [Online]. Available: https://iot.telekom.com/resource/blob/data/175582/cc2ee4be65deac104c1dd2e1e116ca11/nusim-faq.pdf. [Accessed 3 December 2019].

[7] GSM Association, 01 September 2017. [Online]. Available: https://www.gsma.com/newsroom/wp-content/uploads/SGP.21_v2.2.pdf. [Accessed 06 February 2020].

[8] GSM Association, 27 May 2016. [Online]. Available: https://www.gsma.com/newsroom/wp-content/uploads/SGP.02_v3.1.pdf. [Accessed 2 December 2019].

[9] GSM Association, 25 February 2019. [Online]. Available: https://www.gsma.com/newsroom/wp-content/uploads//SGP.01-v4.0.pdf. [Accessed 13 February 2020].

[10] GSM Association, [Online]. Available: https://www.gsma.com/iot/embedded-sim/how-it-works/. [Accessed 26 Februar 2020].

[11] GSM Association, 17 December 2013. [Online]. Available: https://www.gsma.com/iot/wp-content/uploads/2014/01/2.-GSMA-Remote-Provisioning-Architecture-for-Embedded-UICC-Technical-Specification-Version-1.0.pdf. [Accessed 17 February 2020].

[12] GSM Association, June 2019. [Online]. Available: https://www.gsma.com/iot/wp-content/uploads/2019/07/201906-GSMA-NB-IoT-Deployment-Guide-v3.pdf. [Accessed 5 April 2020].

[13] European Telecommunications Standards Institute, June 2012. [Online]. Available: https://www.etsi.org/deliver/etsi_TS/102200_102299/102221/11.00.00_60/ts_102221v110000p.pdf. [Accessed 26 Februar 2020].

[14] European Telecommunications Standards Institute, January 2015. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/131100_131199/131102/12.06.00_60/ts_131102v120600p.pdf. [Accessed 26 February 2020].

[15] Sun Microsystems, Inc., August 2008. [Online]. Available: https://www.oracle.com/technetwork/java/embedded/javacard/documentation/javacard3-whitepaper-149761.pdf. [Accessed March 12 2020].

[16] 1oT, 27 June 2019. [Online]. Available: https://1ot.com/resources/blog/iot-hacking-series-6-what-is-a-sim-applet-and-why-is-it-important-for-iot-m2m. [Accessed 3 April 2020].

[17] A. K. Y. X. B. L. Wai Kay Leong, 2014. [Online]. Available: https://www.comp.nus.edu.sg/~bleong/publications/hotmob14-4gsec.pdf. [Accessed 8 April 2020].

[18] National Institute of Standards and Technology, January 2016. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf. [Accessed 6 April 2020].

[19] Security Research Lab, Security Research Lab, [Online]. Available: https://srlabs.de/bites/sim_attacks_demystified/. [Accessed 30 March 2020].

[20] GSM Association, 16 February 2005. [Online]. Available: https://www.gsma.com/newsroom/wp-content/uploads/2012/12/IR7031.pdf. [Accessed 31 March 2020].

[21] GSM Association, 4 February 2019. [Online]. Available: https://www.gsma.com/newsroom/wp-content/uploads//NG.111-v1.0.pdf. [Accessed 31 March 2020].

[22] AdaptiveMobile, 2019. [Online]. Available: https://simjacker.com/downloads/technicalpapers/AdaptiveMobile_Security_Simjacker_Technical_Paper_v1.01.pdf. [Accessed 30 March 2020].

[23] Ginno Security Laboratory, 21 September 2019. [Online]. Available: https://ginnoslab.org/2019/09/21/wibattack-vulnerability-in-wib-sim-browser-can-let-attackers-globally-take-control-of-hundreds-of-millions-of-the-victim-mobile-phones-worldwide-to-make-a-phone-call-send-sms-to-any-phone-numbers/. [Accessed 30 March 2020].

Appendix 1 – eSIM trace Translated view

This file includes the full translated view of the eSIM trace conducted during the thesis in section 3. The trace includes full eSIM management cycle, download, enabled, disable and delete transactions.

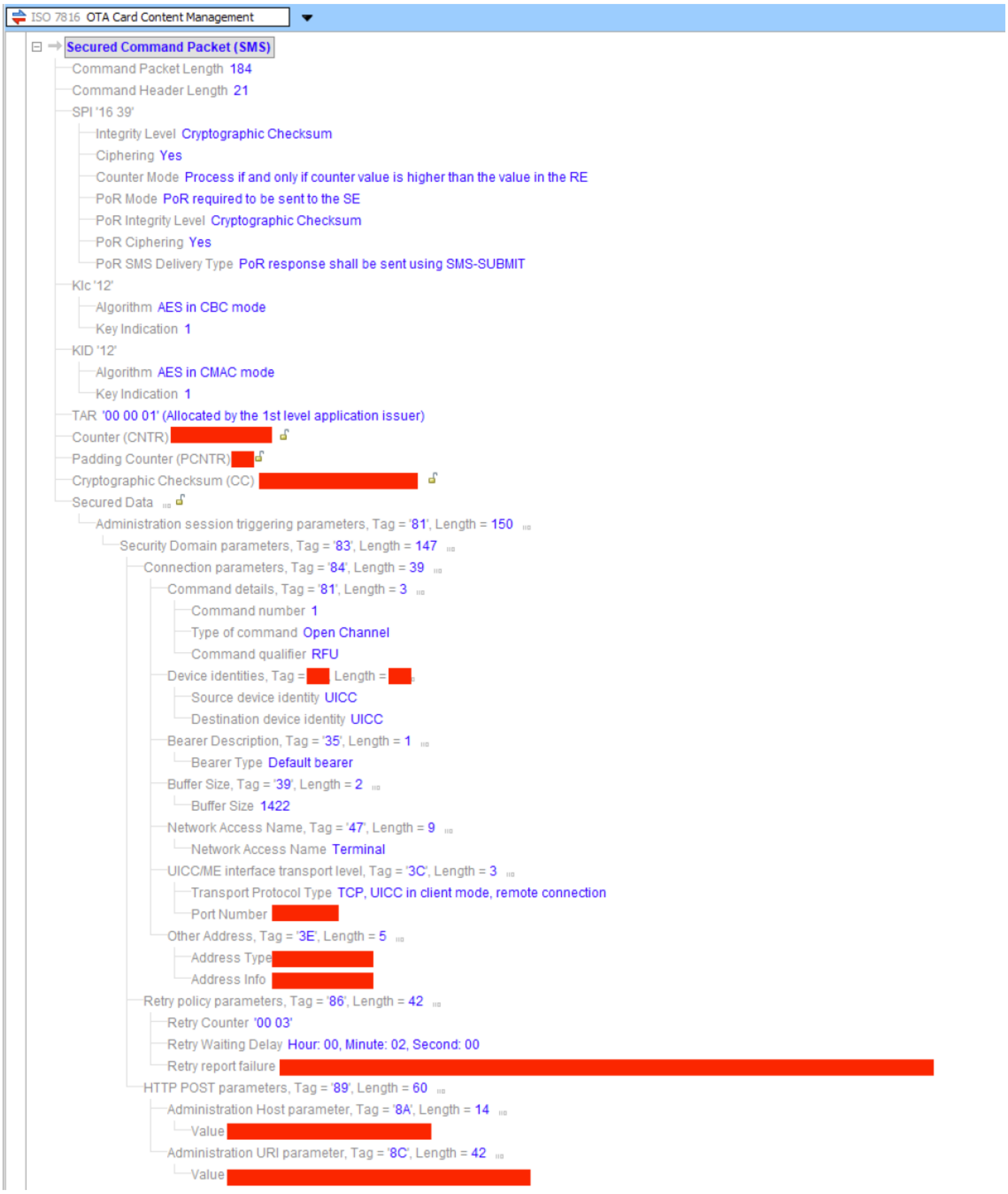
The communication is not decrypted with the card keys because of security concerns.

The file can be accessed with the following link:

https://drive.google.com/open?id=1p6NPluXAvrRHyvrIUL1GTUBYy1I5DZAH

Appendix 2 – eSIM trace OTA Card Content Management view

Below is a part of the trace decrypted OTA Card Content Management view whˇere values of Secure Data parameters have been hidden because of security concerns.



```
Secured Command Packet (SMS)
  Command Packet Length  184
  Command Header Length  21
  SPI '16 39'
    Integrity Level  Cryptographic Checksum
    Ciphering  Yes
    Counter Mode  Process if and only if counter value is higher than the value in the RE
    PoR Mode  PoR required to be sent to the SE
    PoR Integrity Level  Cryptographic Checksum
    PoR Ciphering  Yes
    PoR SMS Delivery Type  PoR response shall be sent using SMS-SUBMIT
  KIc '12'
    Algorithm  AES in CBC mode
    Key Indication  1
  KID '12'
    Algorithm  AES in CMAC mode
    Key Indication  1
  TAR  '00 00 01' (Allocated by the 1st level application issuer)
  Counter (CNTR) [redacted]
  Padding Counter (PCNTR) [redacted]
  Cryptographic Checksum (CC) [redacted]
  Secured Data
    Administration session triggering parameters, Tag = '81', Length = 150
      Security Domain parameters, Tag = '83', Length = 147
        Connection parameters, Tag = '84', Length = 39
          Command details, Tag = '81', Length = 3
            Command number  1
            Type of command  Open Channel
            Command qualifier  RFU
          Device identities, Tag = [redacted] Length = [redacted]
            Source device identity  UICC
            Destination device identity  UICC
          Bearer Description, Tag = '35', Length = 1
            Bearer Type  Default bearer
          Buffer Size, Tag = '39', Length = 2
            Buffer Size  1422
          Network Access Name, Tag = '47', Length = 9
            Network Access Name  Terminal
          UICC/ME interface transport level, Tag = '3C', Length = 3
            Transport Protocol Type  TCP, UICC in client mode, remote connection
            Port Number [redacted]
          Other Address, Tag = '3E', Length = 5
            Address Type [redacted]
            Address Info [redacted]
        Retry policy parameters, Tag = '86', Length = 42
          Retry Counter  '00 03'
          Retry Waiting Delay  Hour: 00, Minute: 02, Second: 00
          Retry report failure [redacted]
        HTTP POST parameters, Tag = '89', Length = 60
          Administration Host parameter, Tag = '8A', Length = 14
            Value [redacted]
          Administration URI parameter, Tag = '8C', Length = 42
            Value [redacted]
```